

# **Innominate mGuard User Manual**

*Software Release 6.0.0*

**Innominate Security Technologies AG  
Albert-Einstein-Str. 14  
D-12489 Berlin  
Tel.: +49 (0)30 6392 3300  
[contact@innominate.com](mailto:contact@innominate.com)  
[www.innominate.com](http://www.innominate.com)**

Copyright © 2008 Innominate Security Technologies AG

March 2008

“Innominate” and “mGuard” are registered trade names of Innominate Security Technologies AG. mGuard technology is protected by patent numbers 10138865 and 10305413, which were granted by the German Patent Office. Additional patents are pending.

This document may not be copied or transferred in whole or in part without prior written approval.

Innominate AG reserves the right to modify this document at any time without prior notice.

Furthermore, Innominate assumes no liability for errors in this manual or for accidental or consequential damages in connection with the delivery, performance or utilization of this document.

This manual may not be photocopied, duplicated or translated into another language, in whole or in part, without the prior written approval of Innominate Security Technologies AG.

Innominate document number: UG206002108-015

# Contents

<b>1</b>	<b>Introduction.....</b>	<b>9</b>
	Network features .....	9
	Firewall features .....	9
	Anti-virus features .....	9
	VPN features .....	10
	Additional features .....	10
	Support .....	10
1.1	Device versions .....	11
	mGuard industrial RS.....	11
	mGuard smart.....	11
	mGuard PCI .....	11
	mGuard blade .....	11
	EAGLE mGuard.....	12
	mGuard delta.....	12
<b>2</b>	<b>Typical Application Scenarios .....</b>	<b>13</b>
	Stealth mode .....	13
	Network router .....	13
	DMZ.....	13
	VPN gateway .....	14
	WLAN over VPN.....	14
	Solving network conflicts .....	15
<b>3</b>	<b>Control Elements and Displays.....</b>	<b>16</b>
3.1	mGuard industrial RS .....	16
3.2	mGuard smart .....	17
3.3	mGuard PCI .....	18
3.4	mGuard blade .....	19
3.5	EAGLE mGuard .....	20
3.6	mGuard delta .....	21
<b>4</b>	<b>Startup .....</b>	<b>22</b>
	Safety	
	instructions .....	22
	General notes regarding usage .....	22
	Startup steps .....	22
	Included in the package.....	23
4.1	Installing the mGuard industrial RS .....	24
	Assembly.....	24
	Disassembly .....	24
	Connections.....	25
4.2	Connecting the mGuard smart .....	30
4.3	Installing the mGuard blade .....	31
	Installing the mGuard bladeBase .....	31
	Installing the mGuard blade .....	31
	Control unit (CTRL slot).....	31
	mGuard blade connection .....	32
4.4	Installing the EAGLE mGuard .....	33
	Terminal block .....	33
	Assembly.....	34
	Startup .....	35
	Network connection .....	35
	Disassembly .....	35
4.5	Connecting the mGuard delta .....	36
4.6	Installing the mGuard PCI .....	37

4.6.1	Selection of Driver mode or Power-over-PCI mode .....	37
	Driver mode .....	37
	Power-over-PCI mode .....	38
4.6.2	Hardware installation .....	40
4.6.3	Driver installation .....	41
	Windows XP .....	41
	Windows 2000 .....	42
	Linux .....	45
<b>5</b>	<b>Preparing the configuration.....</b>	<b>46</b>
5.1	Connection requirements .....	46
	mGuard industrial RS.....	46
	mGuard smart.....	46
	mGuard PCI .....	46
	mGuard blade .....	46
	EAGLE mGuard.....	46
	mGuard delta.....	46
5.2	Local configuration: At startup .....	47
5.2.1	mGuard industrial RS, mGuard smart, mGuard blade and EAGLE mGuard .....	47
	With a configured network interface.....	47
	With a non-configured network interface .....	47
5.2.2	mGuard delta .....	49
5.2.3	mGuard PCI .....	50
	Installing the PCI card.....	50
	Installing the driver .....	50
	Configuring the network interface .....	50
	Default gateway .....	50
5.3	Setting up a local configuration connection .....	52
	Web-based administrator interface .....	52
	After a successful connection setup .....	53
5.4	Remote configuration .....	55
	Requirement .....	55
	Remote configuration.....	55
<b>6</b>	<b>Configuration .....</b>	<b>56</b>
6.1	Operation .....	56
6.2	Management Menu .....	59
6.2.1	Management → System Settings .....	59
	Host .....	59
	Signal contact (only mGuard industrial RS, EAGLE mGuard).....	61
	Time and Date .....	62
	Shell Access .....	65
6.2.2	Management → Web Settings .....	72
	General .....	72
	Access .....	73
6.2.3	Management → Licensing .....	80
	Overview .....	80
	Install.....	81
6.2.4	Management → Update .....	82
	Overview .....	82
	Update .....	83
	AntiVirus Pattern .....	85
6.2.5	Management → Configuration Profiles .....	86
	Configuration Profiles.....	86
	Profiles on the ACA (EAGLE mGuard only).....	87

6.2.6	Management → SNMP .....	89
	Query .....	89
	Trap .....	92
	LLDP .....	97
6.2.7	Management → Central Management .....	98
	Configuration Pull .....	98
6.2.8	Management → Restart .....	101
	Restart .....	101
6.3	Blade Control Menu (control unit only) .....	102
6.3.1	Blade Control → Overview .....	102
6.3.2	Blade Control → Blade 01 to 12 .....	103
	Blade in slot #.....	103
	Configuration .....	104
6.4	Network Menu .....	105
6.4.1	Network → Interfaces .....	105
	General .....	106
	→ Network Mode: Stealth .....	115
	→ Network Mode: Router.....	118
	→ Network Mode: PPPoE .....	120
	→ Network Mode: PPTP .....	121
	→ Network Mode: Modem / Built-in Modem .....	122
	Network Mode → Router, PPPoE, PPTP or Modem / Built-in Modem.....	123
	Ethernet .....	124
	Dial-out .....	126
	Dial-in .....	130
	Modem / Console .....	133
6.4.2	Network → DNS .....	139
	DNS Server .....	139
	DynDNS .....	140
6.4.3	Network → DHCP .....	141
	Internal/External DHCP .....	141
6.4.4	Network → Proxy Settings .....	145
	HTTP(S) Proxy Settings .....	145
6.5	Authentication Menu .....	146
6.5.1	Authentication → Local Users .....	146
	Passwords .....	146
6.5.2	Authentication → Firewall Users .....	148
	Firewall Users .....	148
	RADIUS Servers .....	149
	Access .....	149
	Status .....	149
6.5.3	Authentication → Certificates .....	150
	Creation of certificates .....	152
	Authentication procedure .....	152
	Certificate settings.....	154
	Machine Certificates .....	156
	CA Certificates .....	158
	Remote certificates.....	159
	CRL .....	161
6.6	Network Security Menu (not for blade controller) .....	162
6.6.1	Network Security → Packet Filter .....	162
	Incoming Rules .....	162
	Outgoing Rules.....	164
	Sets of Rules.....	165

	Set of Rules .....	166
	MAC Filtering.....	168
	Advanced .....	169
6.6.2	Network Security → NAT .....	172
	Masquerading.....	172
	Port Forwarding .....	174
6.6.3	Network Security → DoS Protection .....	176
	Flood Protection.....	176
6.6.4	Network Security → User Firewall .....	178
	User Firewall Templates .....	178
	User Firewall → Edit Template .....	178
	General .....	178
	Template users .....	179
	Firewall rules.....	180
6.7	Web Security Menu (not for blade controller) .....	182
6.7.1	Web Security → HTTP .....	182
	Virus Protection .....	182
6.7.2	Web Security → FTP .....	185
	Virus Protection .....	185
6.8	Email Security Menu (not for blade controller) .....	188
6.8.1	Email Security → POP3 .....	188
	Virus Protection .....	188
6.8.2	Email Security → SMTP .....	191
	Virus Protection .....	191
6.9	IPsec VPN Menu (not for blade controller) .....	194
6.9.1	IPsec VPN → Global .....	194
	Options .....	194
	DynDNS Monitoring.....	197
6.9.2	IPsec VPN → Connections .....	198
	Connections.....	198
6.9.3	Defining VPN connection / VPN connection channels .....	200
	General .....	200
	General .....	205
	Authentication .....	207
	Firewall .....	213
	IKE Options .....	215
6.9.4	IPsec VPN → L2TP over IPsec .....	216
	L2TP Server .....	217
6.9.5	IPsec VPN → IPsec Status .....	217
6.10	SEC-Stick Menu .....	220
6.10.1	Global .....	220
	Access .....	220
6.10.2	Connections .....	222
	SEC-Stick Connections.....	222
6.11	QoS Menu .....	224
6.11.1	Ingress Filter .....	224
	Internal / External.....	224
6.11.2	Egress Queues .....	227
	Internal / External / External 2 / Dial-in.....	227
6.11.3	Egress Queues (VPN) .....	228
	VPN via Internal / VPN via External / VPN via External 2 / VPN via Dial-in ...	228
6.11.4	Egress Rules .....	230
	Internal / External / External 2 / Dial-in.....	230
6.11.5	Egress Rules (VPN) .....	231

	VPN via Internal / VPN via External / VPN via External 2 / VPN via Dial-in ...	231
6.12	Redundancy Menu .....	234
6.12.1	Firewall Redundancy .....	234
	Redundancy.....	235
	ICMP Checks .....	236
6.12.2	Ring / Network Coupling .....	237
	Ring / Network Coupling .....	237
6.13	Logging Menu .....	238
6.13.1	Logging → Settings .....	238
	Remote Logging.....	238
6.13.2	Logging → Browse local logs .....	239
	Log entry categories.....	239
6.14	Support Menu .....	243
6.14.1	Support → Tools .....	243
	Ping Check .....	243
	Traceroute .....	243
	DNS Lookup .....	244
	IKE Ping.....	244
6.14.2	Support → Advanced .....	245
	Hardware .....	245
	Snapshot .....	245
6.15	CIDR (Classless Inter-Domain Routing) .....	246
6.16	Network Example .....	247
<b>7</b>	<b>The Rescue Button – Restarting, the Recovery Procedure and Flashing Firmware.....</b>	<b>248</b>
7.1	Performing a restart .....	248
7.2	Performing a recovery .....	248
7.3	Flashing the firmware .....	249
	Requirements for flashing the firmware: DHCP and TFTP server.....	251
7.3.1	Installing DHCP and TFTP servers in Windows or Linux .....	252
	In Windows .....	252
	In Linux .....	253
<b>8</b>	<b>Glossary .....</b>	<b>254</b>
	Asymmetrical encryption .....	254
	DES / 3DES.....	254
	AES .....	254
	CA certificate .....	254
	Client / Server .....	255
	Datagram .....	255
	Default route.....	255
	DynDNS provider .....	256
	IP address .....	256
	IPsec .....	257
	Subject, certificate.....	258
	NAT (Network Address Translation).....	259
	Port number.....	259
	Proxy .....	259
	PPPoE.....	259
	PPTP.....	259
	Router .....	259
	Trap .....	260
	X.509 certificate .....	260
	Protocol, communication protocol .....	260
	Service provider .....	260
	Spoofing, anti-spoofing .....	260

Symmetrical encryption .....	261
TCP/IP (Transmission Control Protocol/Internet Protocol).....	261
VLAN.....	261
VPN (Virtual Private Network) .....	261
<b>9 Technical Data.....</b>	<b>262</b>
General .....	262
mGuard industrial RS.....	262
EAGLE mGuard.....	263

# 1 Introduction

The mGuard protects IP data connections. In doing this, the device incorporates the following functions:

- Network card (mGuard PCI), switch (mGuard delta).
- VPN router (VPN - Virtual Private Network) for the secure transfer of data via public networks (hardware-based DES, 3DES and AES encryption, IPsec protocol).
- Configurable firewall for protection against unauthorized access.  
The dynamic packet filter inspects data packets using the source and destination addresses and blocks undesired traffic.
- Anti-virus protection with support for HTTP, FTP, SMTP and POP3 protocols.

The device can be easily configured using a web browser.

---

For further information, consult:

- The product data sheets on the CD delivered with the device (if CD is included) or on
  - the Innominate website: [www.innominate.de](http://www.innominate.de) (including additional documents)
- 

## Network features

- Stealth (Auto, Static, Multi), Router (Static, DHCP Client), PPPoE (for DSL), PPTP (for DSL) and Modem modes
- VLAN
- DHCP Server/Relay on external and internal network interfaces
- DNS cache on the internal network interface
- Administration using HTTPS and SSH
- Optional rewrite of DSCP/TOS values (Quality of Service values)

## Firewall features

- Stateful Packet Inspection
- Anti-spoofing
- IP filter
- L2 filter (only in Stealth mode)
- NAT with FTP, IRC and PPTP support (only in Router modes)
- 1:1 NAT (only in *Router* network mode)
- Port forwarding (not in *Stealth* network mode)
- Individual firewall rules for different users (user firewall)
- Individual rule records as action (target) of firewall rules (apart from user or VPN firewall)
- Firewall throughput: max. 99 MBit/s

## Anti-virus features

- ClamAV virus protection
- Supported protocols: HTTP, FTP, POP3 and SMTP (sending)
- The virus filter can decompress the following formats:
  - ZIP
  - RAR
  - GZIP
  - BZIP2
  - TAR
  - MS OLE2
  - MS CHM (compressed HTML)
  - MS SZDD
  - UPX
  - FSG

- Petite

## **VPN features**

- Protocol: IPsec (Tunnel and Transport mode)
- IPsec encryption in hardware with DES (56 Bit), 3DES (168 Bit), AES (128, 192, 256 Bit)
- Packet authentication: MD5, SHA-1
- Internet Key Exchange (IKE) with Main and Quick mode
- Authentication using:
  - Pre-Shared Key (PSK)
  - X.509v3 certificates:
    - Public Key Infrastructure (PKI) with Certification Authority (CA), optional Certificate Revocation List (CRL) and filter options according to subject
- or
  - Remote certificate (e.g. self-signed certificates)
- Recognition of changing remote peer IP addresses using DynDNS
- NAT Traversal (NAT-T)
- Dead Peer Detection (DPD): Recognition of IPsec connection breaks
- IPsec/L2TP server: Connections from IPsec/L2TP clients
- IPsec firewall and 1:1 NAT
- Default route over VPN
- Forwarding of data between VPNs (hub and spoke)
- Up to 250 VPN tunnels
- VPN throughput of max. 35 MBit/s (266 MHz mGuard) and 70 MBit/s (533 MHz mGuard)

## **Additional features**

- MAU management
- Remote Logging
- Router / Firewall redundancy
- LLDP
- Administration using SNMP v1-v3 and Innominate Device Manager (IDM)
- Quality of Service (QoS)
- PKI support for HTTPS/SSH Remote Access

## **Support**

Please contact your local dealer if problems occur with the mGuard.  
Additional information on the device and relevant changes, plus release notes and software updates can be found on our website: <http://www.innominate.com/>

## 1.1 Device versions

mGuard is available in the following device versions, which all have largely identical functions. All devices can be utilized regardless of the processor technology and operating system used by the connected computers.

### mGuard industrial RS

The mGuard industrial RS is available in three different device versions: With built-in modem, with built-in ISDN terminal adaptor or without both devices. It can then be used as a firewall/VPN router over ethernet or serial dial-up network connections. “RS” means that this device is especially suited for secure Remote Services (remote diagnosis, remote configuration, telephone services). The device is designed for assembly on DIN rails (according to DIN EN 50 022) and is therefore especially suited for use in industrial environments. VPN tunnels can be initiated using the software or hardware switch. Redundant power supplies are supported (9-36 V DC).



### mGuard smart

Smallest device model. It can be plugged easily between the computer or local network (on LAN port of mGuard) and an available router (on WAN port of mGuard), without having to change existing system configurations or driver installations. Designed for instant use in the office or when travelling.



### mGuard PCI

This card can be plugged into a PCI slot and provides the connected computer with all mGuard functions in *Driver mode*. It can also be used as a normal network card. An existing network card or another local computer / local network can be connected in *Power-over-PCI mode*.



### mGuard blade

The mGuard bladePack includes the mGuard bladeBase. This can be easily installed into standard 3 U racks (19 inches) and can accommodate up to 12 mGuard blades. This version is thus ideally suited for use in an industrial environment, where it can protect several server systems individually and independently of one another. An additional serial port enables remote configuration using a telephone dial-up connection or a terminal.



## **EAGLE mGuard**

The EAGLE mGuard is designed for assembly on DIN rails (according to DIN EN 50 022) and is therefore especially suited for use in industrial environments. Additional application options are provided by the optional configuration connection and the option for establishing a telephone dial-up connection via the V.24 interface.



## **mGuard delta**

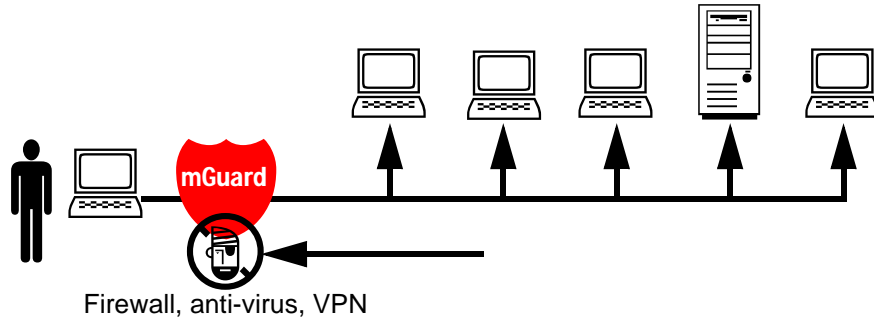
This model is a compact LAN switch (Ethernet / Fast Ethernet) designed for connecting up to 4 LAN segments. This device is especially suited for logically segmented network environments where locally connected computers / networks share mGuard functions. An additional serial port enables configuration using a telephone dial-up connection or a terminal. The mGuard delta has a robust metal housing, making it suitable as a desktop device or for use in wiring storage rooms.



## 2 Typical Application Scenarios

Some of the more common application scenarios are detailed below.

### Stealth mode

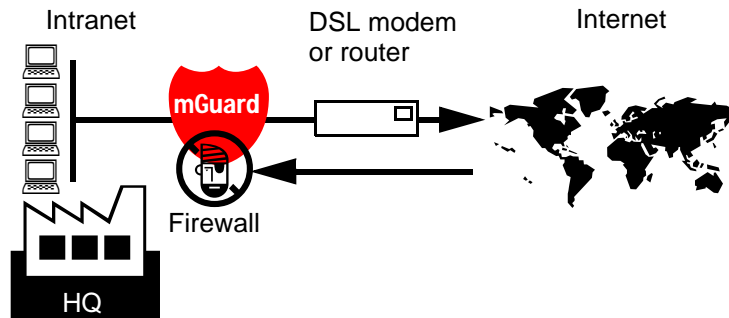


In *Stealth* mode (factory default), the mGuard can be installed between an individual computer and the rest of the network.

The settings for firewall, anti-virus and VPN can be made using a web browser under the URL <https://1.1.1.1/>.

No configuration changes are required on the computer itself.

### Network router



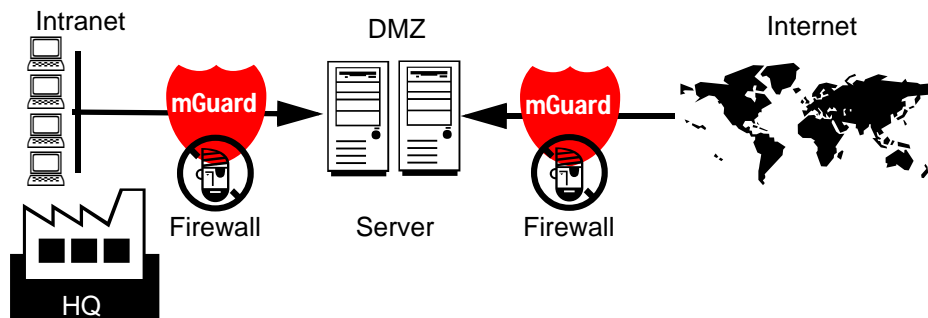
The mGuard can provide an Internet connection for a group of computers whilst protecting the company network using the firewall.

One of the following network modes may be used here:

- *Router*, if Internet access is established via a DSL router or dedicated line.
- *PPPoE*, if Internet access is established via a DSL modem using the PPPoE protocol (e.g. in Germany).
- *PPTP*, if Internet access is established via a DSL modem using the PPTP protocol (e.g. in Austria).
- *Modem*, if Internet access is established via a serial connected modem (compatible with Hayes or AT instruction sets).

The mGuard must be set as the default gateway on computers placed in the Intranet.

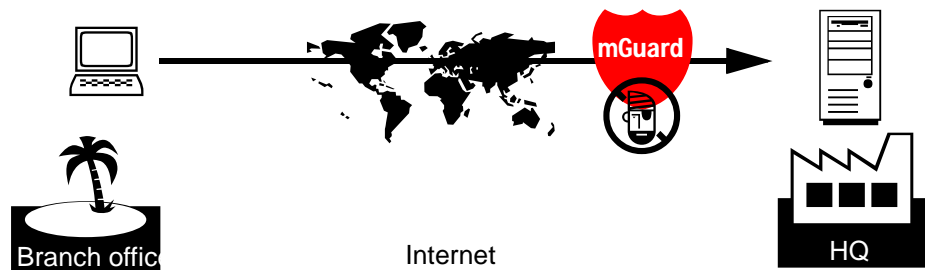
### DMZ



A DMZ (Demilitarized Zone) is a protected network that sits between two other networks. For example, a company website may be inside a DMZ, granting FTP write access to computers in the intranet and HTTP read-only access to both networks (i.e. also over the Internet).

IP addresses within a DMZ can be public or private. In the latter case, the mGuard connected to the Internet forwards the connections using “port forwarding” to the private addresses within the DMZ.

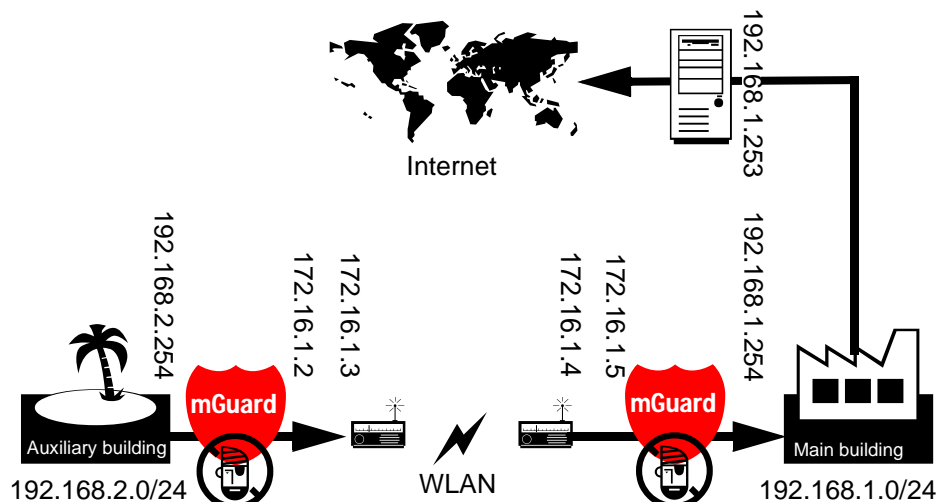
### VPN gateway



Encrypted access to the company network should be provided to employees at home or whilst travelling. The mGuard thereby takes on the role of the VPN gateway.

On external computers, IPsec capable VPN client software must be installed, the operating system must support this function (e.g. Windows 2000/XP) or an mGuard must be installed.

### WLAN over VPN



Two company buildings should be connected to each other over an IPsec protected WLAN connection. The auxiliary building should also be able to use the Internet connection of the main building.

In this example, the mGuards were switched to *Router mode* and a separate network with addresses of 172.16.1.x was created for the WLAN.

As Internet access should also be available via the VPN from the auxiliary building, a “Default route over VPN” is configured here.

#### Auxiliary building tunnel configuration

Connection type	Tunnel (Network <-> Network)
Local network address	192.168.2.0/24
Remote network address	0.0.0.0/0

The appropriate connection counterpart is configured in the main building:

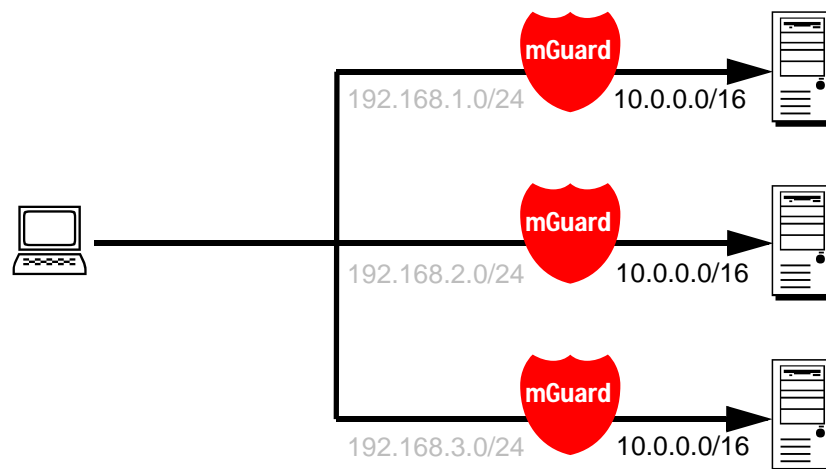
**Main building tunnel configuration**

Connection type	Tunnel (Network <-> Network)
Local network	0.0.0.0
Remote network address	192.168.2.0/24

The default route of an mGuard is usually directed over the WAN port, but in this case the Internet is accessible via the LAN port:

**Main building default gateway**

IP of default gateway	192.168.1.253
-----------------------	---------------

**Solving network conflicts**

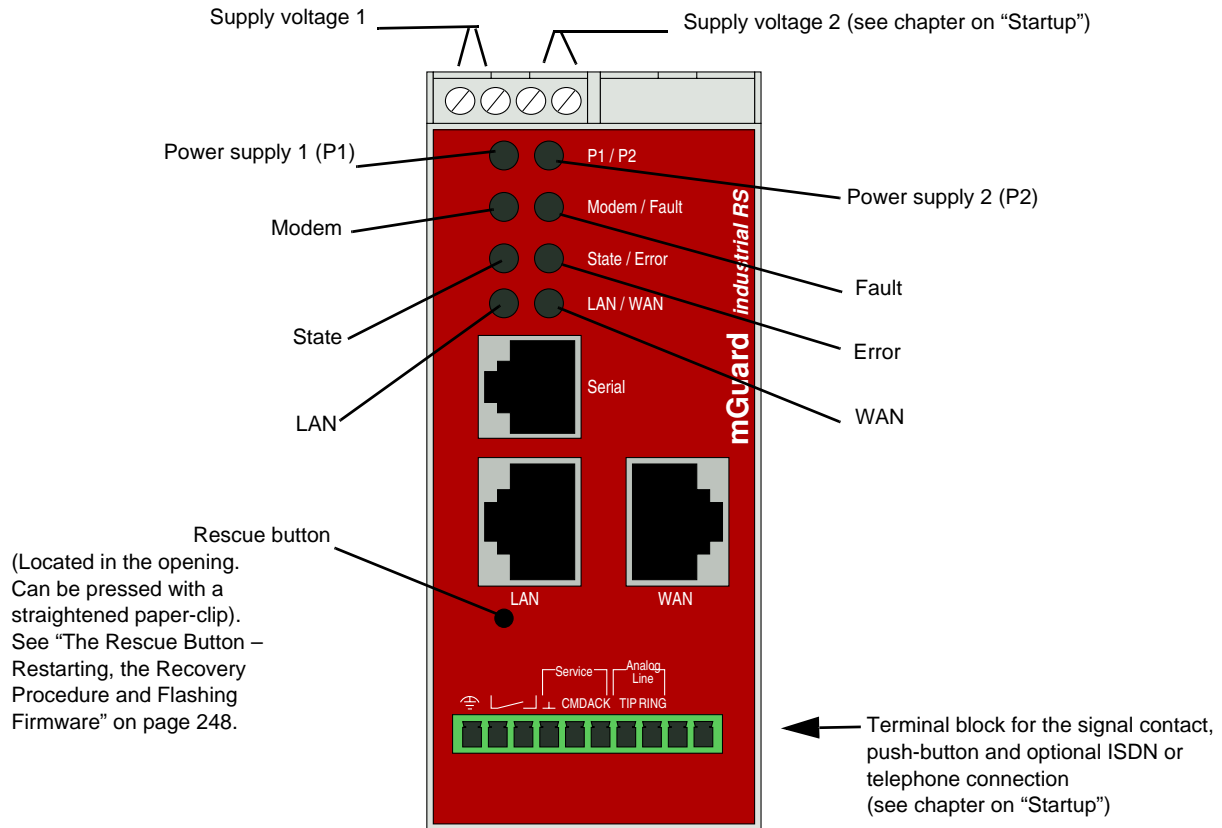
In the illustration above, the networks on the right-hand side should be accessible from the network or the computer on the left-hand side. However, due to historical or technical reasons, the computer networks overlap on the right-hand side.

The conflict can be solved by rewriting these networks using the mGuard 1:1 NAT feature.

(1:1 NAT can be used in normal routing and in IPsec tunnels).

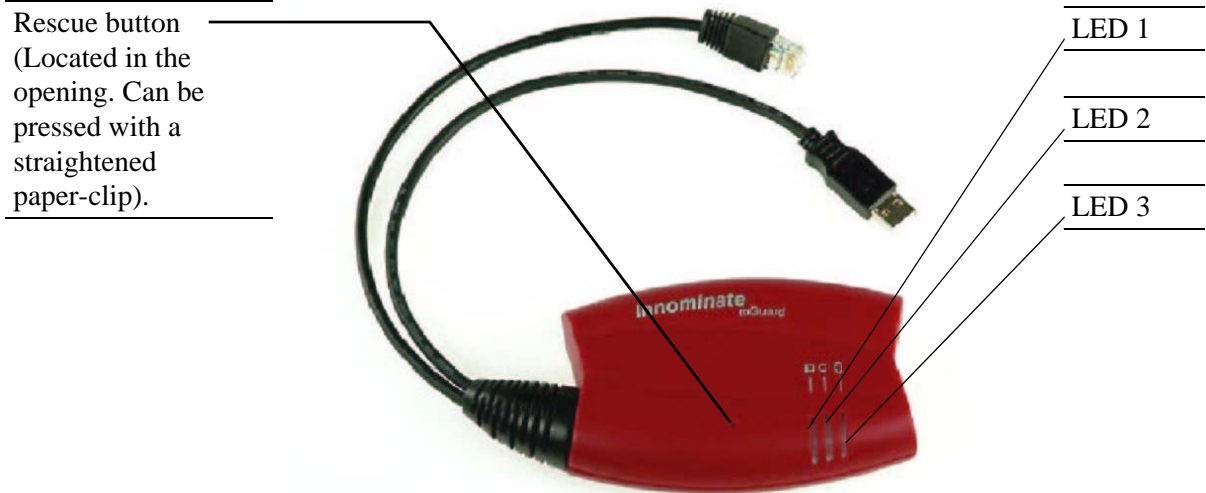
### 3 Control Elements and Displays

#### 3.1 mGuard industrial RS



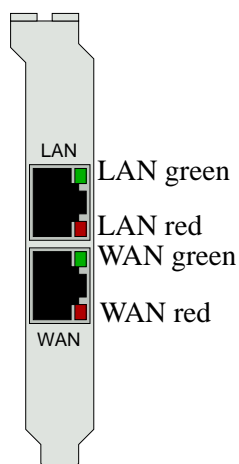
	State	Meaning
P1	Green	Power supply 1 is active
P2	Green	Power supply 2 is active
Modem	Green	Connection established over modem
Fault	Red	The signal contact is open due to an error – see "Installing the mGuard industrial RS" on page 24, under "Signal contact". (The signal contact is interrupted during a reboot)
State	Green flashing	<b>Heartbeat.</b> The device is correctly connected and functioning.
Error	Red flashing	<b>System error.</b> Reboot the system. ☒ Press the Rescue button briefly (1.5 seconds). OR Disconnect the device from its power supply briefly and then reconnect it. If the error continues to occur, start the <i>Recovery procedure</i> (see "Performing a recovery" on page 248) or contact the support department.
State + Error	Flashing alternately (green-red)	<b>Boot process.</b> After connecting the device to the power supply. The LED switches to heartbeat mode after a few seconds.
LAN	Green	<b>Ethernet status.</b> Shows the status of the LAN and WAN ports. As soon as the device is connected to the relevant network, the LEDs are illuminated continuously to indicate the presence of a network connection over LAN or WAN. The LEDs are extinguished briefly when data packets are transferred.
WAN	Green	

## 3.2 mGuard smart



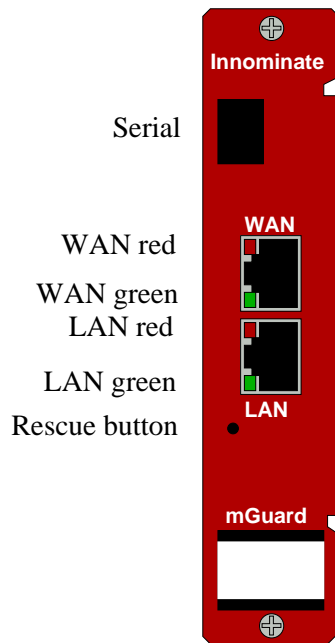
	Color	State	Meaning
<b>2</b>	Red/green	Red/green flashing	<b>Boot process.</b> After connecting the device to the power supply. The LED switches to heartbeat mode after a few seconds.
	Green	Flashing	<b>Heartbeat.</b> The device is correctly connected and functioning.
	Red	Flashing	<b>System error.</b> <input checked="" type="checkbox"/> Reboot the system. Press the Rescue button briefly (1.5 seconds) OR Disconnect the device from its power supply briefly and then reconnect it. If the error continues to occur, start the <i>Recovery</i> procedure (see “Performing a recovery” on page 248) or contact the support department.
<b>1 and 3</b>	Green	On or flashing	<b>Ethernet status.</b> LED 1 shows the status of the LAN port. LED 3 shows the status of the WAN port. As soon as the device is connected, the LEDs are illuminated continuously to indicate the presence of a network connection. The LEDs are extinguished briefly when data packets are transferred.
<b>1, 2, 3</b>	Various LED illumination codes		<b>Recovery mode.</b> After pressing the <b>Rescue</b> button. See “The Rescue Button – Restarting, the Recovery Procedure and Flashing Firmware” on page 248.

### 3.3 mGuard PCI



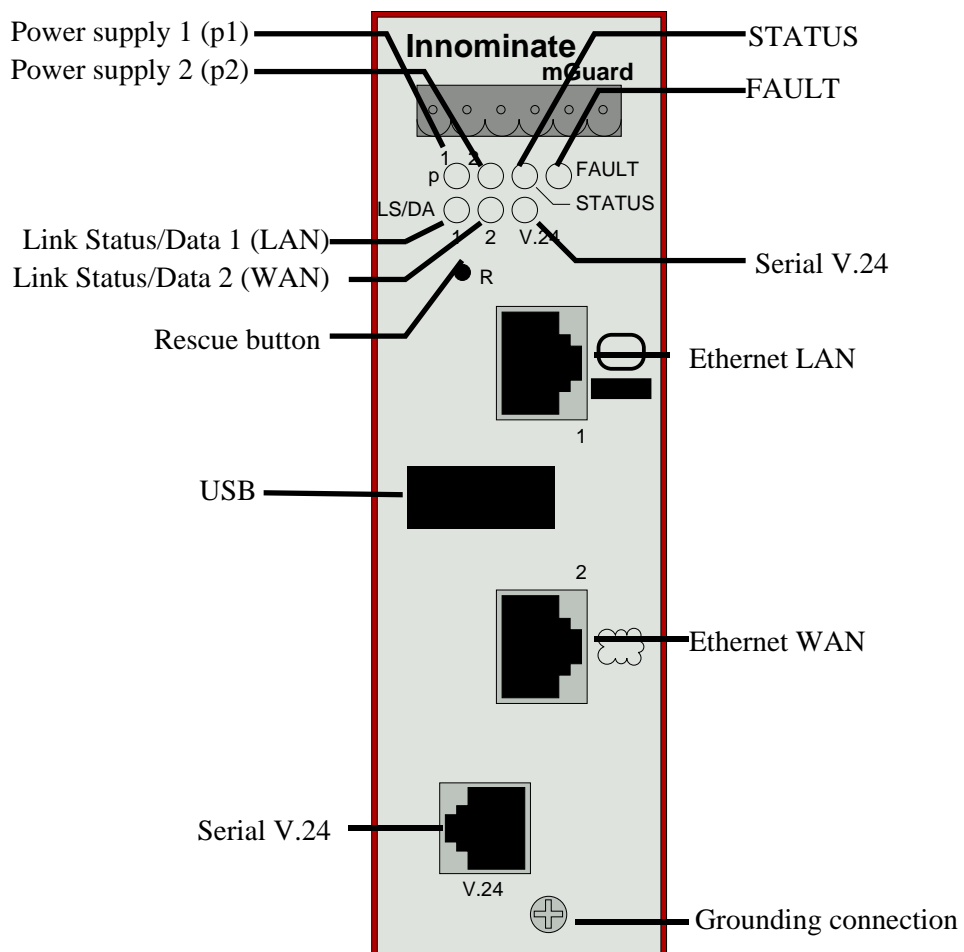
LEDs	State	Meaning
WAN red, LAN red	Flashing	<b>Boot process.</b> After starting or restarting the computer.
WAN red	Flashing	<b>System error.</b> <input checked="" type="checkbox"/> Reboot the system. Press the <b>Rescue</b> button briefly (1.5 seconds). OR Reboot the computer. If the error continues to occur, start the <i>Recovery</i> procedure (see “Performing a recovery” on page 248) or contact the support department.
WAN green, LAN green	On or flashing	<b>Ethernet status.</b> Shows the status of the LAN and WAN interface. As soon as the device is connected, the LEDs are illuminated continuously to indicate the presence of a network connection. The LEDs are extinguished briefly when data packets are transferred.
WAN green, WAN red, LAN green	Various LED illumination codes	<b>Recovery mode.</b> After pressing the <b>Rescue</b> button. See “The Rescue Button – Restarting, the Recovery Procedure and Flashing Firmware” on page 248.

### 3.4 mGuard blade



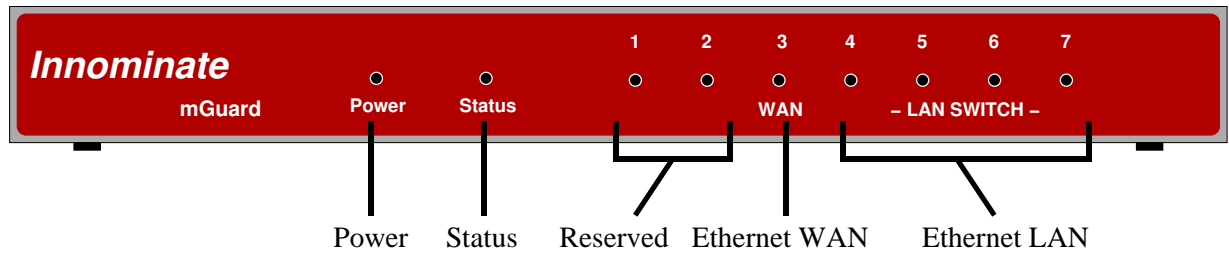
	State	Meaning
<b>WAN red, LAN red</b>	Flashing	<b>Boot process.</b> After starting or restarting the computer.
<b>WAN red</b>	Flashing	<b>System error.</b> <input checked="" type="checkbox"/> Reboot the system. Press the <b>Rescue</b> button briefly (1.5 seconds). If the error continues to occur, start the <i>Recovery</i> procedure (see “Performing a recovery” on page 248) or contact the support department.
<b>WAN green, LAN green</b>	On or flashing	<b>Ethernet status.</b> Shows the status of the LAN and WAN interface. As soon as the device is connected, the LEDs are illuminated continuously to indicate the presence of a network connection. The LEDs are extinguished briefly when data packets are transferred.
<b>WAN green, WAN red, LAN green</b>	Various LED illumination codes	<b>Recovery mode.</b> After pressing the <b>Rescue</b> button. See “The Rescue Button – Restarting, the Recovery Procedure and Flashing Firmware” on page 248.

### 3.5 EAGLE mGuard



	State	Meaning
<b>p1, p2</b>	Green	Power supply 1 or 2 is active
<b>STATUS</b>	Green flashing	The mGuard is booting
	Green	The mGuard is ready
	Yellow	The mGuard is ready and is Redundancy Master
	Yellow/green flashing	The mGuard is ready and is Redundancy Slave
<b>FAULT</b>	Red	The signal contact is open after an error. See “Installing the EAGLE mGuard” on page 33, under “Signal contact”.
<b>LS/DA 1/2 V.24</b>	Green	Link detected
	Yellow flashing	Data transfer

### 3.6 mGuard delta



	State	Meaning
<b>Power</b>	On	The power supply is active
<b>Status</b>	On	The mGuard is booting
	Heartbeat (flash, flash, pause, ...)	The mGuard is ready
<b>1,2</b>	-	Reserved
<b>3 (WAN)</b>	On	Link detected
	Flashing	Data transfer
<b>4-7 (LAN)</b>	On	Link detected
	Flashing	Data transfer

## 4 Startup

### Safety instructions

In order to operate properly, and to help ensure the safety of persons and property, the mGuard must be correctly installed, operated and maintained. Use the mGuard only in the appropriate manner and only for appropriate purposes.

Only connect the mGuard's network interfaces to LAN installations. **Warning!** Some telephone lines also use RJ45 jacks, which must not be connected to the RJ45 jacks of the mGuard.



#### Warning!

This is a Class A device, which may cause radio interference in a living area, in which case the operator may be requested to take appropriate measures.

Please also note the further device specific safety instructions within the following sections.

### General notes regarding usage

- mGuard PCI: Your PC must have a free PCI slot (3,3 V or 5 V).
- Use a soft cloth to clean the device housing. Do not use abrasive solvents and liquids!
- Ambient environmental conditions:  
0 to +40 °C (smart, blade, delta), 70 °C (PCI), 55 °C (mGuard industrial RS, EAGLE mGuard)
- Max. 90% non-condensing humidity (mGuard industrial RS, EAGLE mGuard: 95%).
- To avoid overheating, do not expose to direct sunlight or other heat sources.
- Do not bend connection cables. Only use the network connector for connection to a network.

### Startup steps

To start the device, perform the following steps in the listed order:

Step	Action	Page
1	Check the package contents and read the Release Notes	"Included in the package" on page 23
2	Connect the device	"Installing the mGuard industrial RS" on page 24 "Connecting the mGuard smart" on page 30 "Installing the mGuard blade" on page 31 "Installing the EAGLE mGuard" on page 33 "Connecting the mGuard delta" on page 36 "Installing the mGuard PCI" on page 37
3	Configure the device as required. Proceed through the various options given in the mGuard configuration menus. Please consult the relevant sections of this manual for more information regarding the required options and settings for your operating environment.	"Local configuration: At startup" on page 47

**Included in the package**

Before setting the device, check that the package is complete:

- The device *mGuard industrial RS*, *mGuard blade*, *delta*, *PCI*, *smart* or *EAGLE mGuard*
- Quick Installation Guide

**The mGuard industrial RS also contains:**

- Terminal block for the power supply (attached)
- Terminal block for the signal contact, push-button and optional ISDN or telephone connection

**The mGuard bladePack also contains:**

- 19" mGuard bladeBase
- An mGuard blade as controller
- Two power supplies
- Two power cables
- 12 place holders
- 12 handle plates M1 to M12
- Screws for installing the bladeBase

**The mGuard delta also contains:**

- A 5 V DC power supply
- Two UTP ethernet cables

## 4.1 Installing the mGuard industrial RS

### Assembly

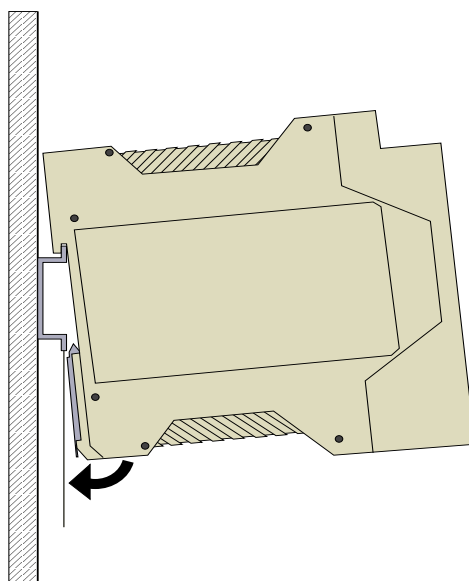
The device is delivered in a ready-to-operate condition. The following procedure is required for the assembly and connection process:

1. Pull the terminal block from under the mGuard industrial RS and connect the contact lines and other connections according to their use – see below under “Connection options on lower terminal block” on page 26.

When the device is assembled, set the wired terminal block back on the DIN rail.

2. Attach the mGuard industrial RS onto a 35 mm DIN rail according to DIN EN 50 022.

Attach the upper snap-on guide of the mGuard industrial RS to the DIN rail and press it down until it locks into position.



3. Connect the supply voltage on the upper side of the terminal block – see below under “Supply voltage” on page 25.
4. Make the necessary network connections on the LAN or WAN port – see below under “Network connection” on page 25.
5. If necessary, connect the serial port of the relevant device – see below under “Serial Port” on page 29.

☒ The device forwards the grounding from the DIN rail through to the left contact (grounding connection) on the lower terminal block.

☒ Do not open the housing.

☒ The shielding ground of the connectable twisted pair lines is electrically connected to the front faceplate.



### Warning!

This is a Class A device, which may cause radio interference in residential areas, in which case the operator may be requested to take appropriate measures. If installed in a living area or office environment, the mGuard industrial RS must be operated exclusively in switch cabinets with fire protection characteristics in accordance with EN 60950-1.

### Disassembly

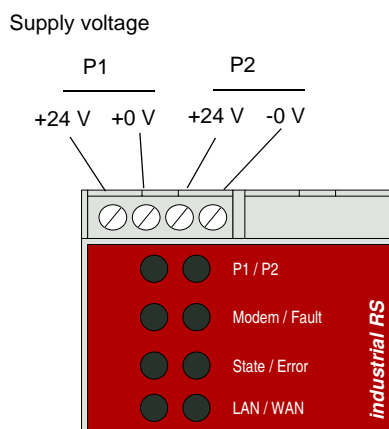
Remove or disconnect the connections.

To remove the mGuard industrial RS from the DIN rail, insert a screwdriver horizontally under the housing into the locking slide, pull it (without tipping the screwdriver) downwards and lift the mGuard industrial RS upwards.

## Connections

### Supply voltage

Connection of the **supply voltage** is made using a terminal block with a screw mechanism. This is found on the top of the device.



**Safety notice:** The Innominate mGuard industrial RS is intended for operation with direct 9 - 36V DC/SELV max. 0.5A. Its power supply connections and signaling contact may only be connected to SELV circuits with voltage restrictions in accordance with EN 60950-1.

### Operating voltage

NEC class 2 power source 12 V DC or 24 V DC -25% +33% safety extra-low voltage (SELV/PELV, decoupled redundant entries), max. 5 A. Buffer time min. 10ms at 24 V DC.

### Redundant power supply

Redundant power supplies are supported. Both inputs are decoupled. There is no load distribution. With a redundant supply, only the power supply unit with the higher output voltage supplies the mGuard industrial RS. The supply voltage is electrically isolated from the housing.

☒ In case of a non-redundant voltage supply, the mGuard industrial RS indicates the failure of the supply voltage over the signal contact (see below). You can prevent this message by connecting the supply voltage to both inputs.

### Network connection



**Safety notice:** Only connect the mGuard's network interfaces to LAN installations. For network connections, Ethernet cables with strain relief boots should be used. Unused Ethernet jacks should be covered with the dummy plugs that are contained in the package. Some telephone lines also use RJ45 jacks, which must not be connected to the RJ45 jacks of the mGuard.

#### LAN Port:

Connect the local computer or network to the mGuard LAN port using a UTP ethernet cable (CAT 5).

If the computer is already connected to a network, then patch the mGuard *between* the existing network connections.

Please note that initial configuration can only be made over the LAN interface. The mGuard industrial RS firewall rejects all IP traffic from the WAN to the LAN interface.

#### WAN Port:

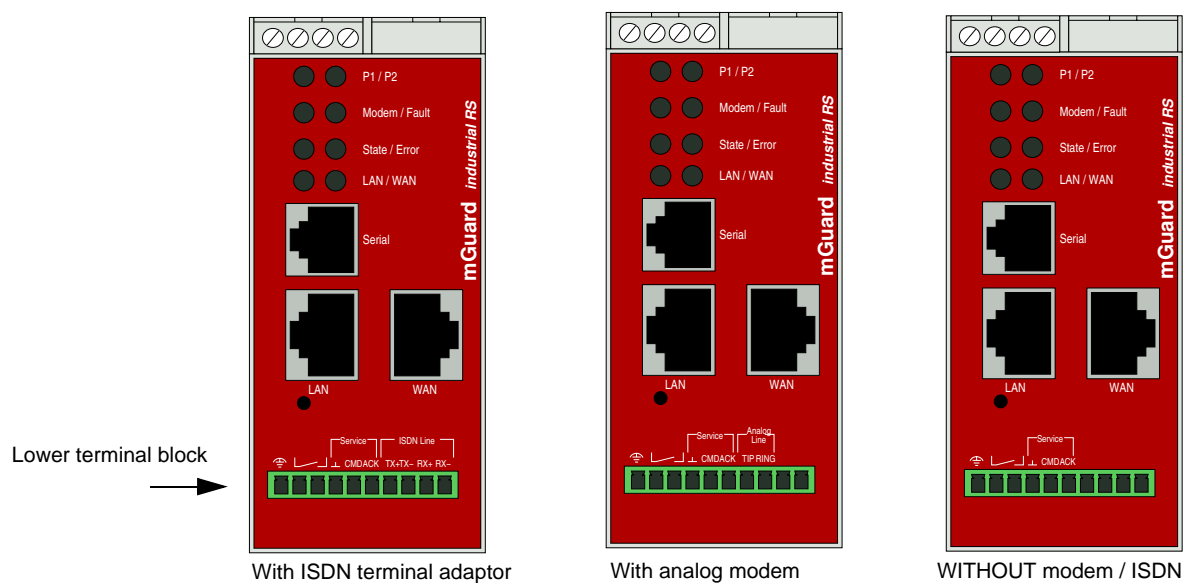
Socket for connection to an external network, e.g. WAN, Internet.

Connections to the remote device or network are established over this network. Use a UTP cable (CAT 5).

- ☒ Additional driver installation is not necessary.
- ☒ For security reasons, we recommend that you change the default Root and Administrator passwords during the first configuration.

### Connection options on lower terminal block

The mGuard industrial RS is available in three different versions. These can be distinguished through the connection options on the bottom part of the terminal bar:



### mGuard industrial RS **WITHOUT** modem / ISDN terminal adaptor:

Lower area on front faceplate with terminal block

Function grounding

Signal contact  
(interrupted if errors occur)

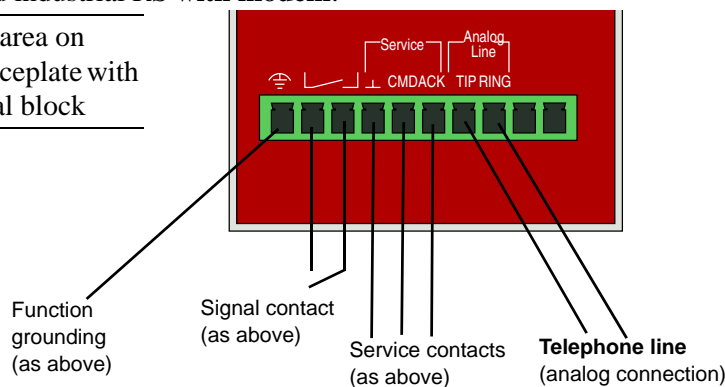
Push-button  
OR on/off switch

Signal LED (20 mA)

**Service contacts:**  $\perp$  CMD, ACK  
(for establishing a predefined VPN connection)

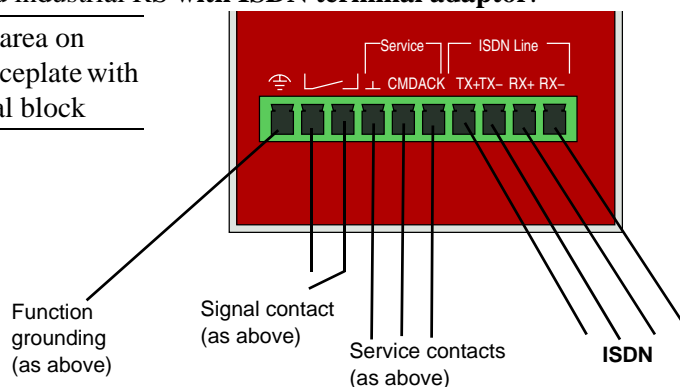
### mGuard industrial RS with modem:

Lower area on front faceplate with terminal block



### mGuard industrial RS with ISDN terminal adaptor:

Lower area on front faceplate with terminal block



### Function grounding

Can be used by the operator. This connection is electrically connected to the rear side of the mGuard industrial RS. Grounding of the mGuard industrial RS is made during assembly on a DIN rail with a metal clamp. The DIN rail is connected to the rear side of the mGuard. The DIN rail must be electrically grounded.

### Signal contact



**Safety notice:** The signaling contact may only be connected to SELV circuits with voltage restrictions in accordance with EN 60950-1.

The signal contact is used to monitor the functions of the mGuard industrial RS and thereby allows remote diagnosis. The following is reported through interruption of the contact using potential-free signal contacts (relay contact, closed current circuit):

- The failure of at least one of the two supply voltages.
- A power supply shortfall for the mGuard industrial RS (supply voltage 1 and/or 2 smaller than 9 V).
- The faulty link status of at least one port. The link state report on the mGuard industrial RS can be masked on a port-by-port basis using the management software.
- No connection monitoring is offered in the factory default condition.
- Self-test error.

☒ The signal contact is interrupted during a reboot until the mGuard is fully operative. This also applies when the signal contact is set manually to *Closed* in the software configuration.

## Service contacts



**Safety notice:** The service contacts ( $\perp$ , CMD, ACK) must not be connected to an external power supply, but rather connected as described here in detail.

A push-button or an on/off switch (e.g. key switch) can be connected over the service contacts CMD and  $\perp$ . A customary LED (up to 3.5 V) or alternatively a corresponding optocoupler can be connected over the service contacts ACK (+) and  $\perp$  (-). The contact is short-circuit-proof and supplies 20 mA at most. See diagram above for wiring. The push-button or on/off switch is used for establishing and disabling a previously defined VPN connection, whilst the LED displays the status of the VPN connection.

See “IPsec VPN → Global” on page 194 under **Options**.

### Operating a connected push-button:

To establish a VPN connection, press and hold the push-button for a few seconds until the signal LED flashes. Only release the push-button at this point. The flashing LED signals that the mGuard has received the command for establishing a VPN connection and has started the connection process. The LED lights up continuously as soon as the VPN connection is established.

To disable the VPN connection, press and hold the push-button for a few seconds until the signal LED flashes or goes out. Only release the push-button at this point.

The VPN connection is disabled when the signal LED no longer lights up.

### Operating a connected on/off switch:

To establish the VPN connection, turn the switch to ON.

To disable the VPN connection, turn the switch to OFF.

**Signal LED:** If the signal LED is set to OFF, then the defined VPN connection is disabled. Cause: VPN connection not established or failed due to errors. If the signal LED is set to ON, then the VPN connection is established. If the signal LED flashes, then the VPN connection is being established or disabled.

## Analog line (with built-in modem)



**Safety notice:** The analog lines (TIP, RING) may only be connected to the appropriate telephone line.

The TIP and RING contacts are used for connection to a telephone landline (analog connection).

The following descriptions are used in Germany for the contact details on the frontplate.

TIP = a | RING = b

## ISDN line (with built-in ISDN terminal adaptor)



**Safety notice:** The ISDN contacts (TX+, TX-, RX+, RX-) must only be connected to an ISDN S0 bus.

The TX+, TX-, RX-, and RX+ contacts are used for connection to the ISDN and display the mGuard industrial RS as an ISDN participant. The following table describes the pole (contact) assignments for 8-pole connections for plugs and jacks, in example RJ45.

Pole Number	TE (mGuard)
3	TX+

Pole Number	TE (mGuard)
4	RX+
5	RX-
6	TX-

## Serial Port



**Safety notice:** The serial interface (RJ12 jack) must not be connected directly to telephone lines. A serial cable with RJ12 plug has to be used to connect a serial terminal or a modem. The maximum length of the serial cable is 30m.

The serial port (serial interface) can be used as follows:

- a) For configuration of the mGuard over the serial interface. There are two possibilities here:

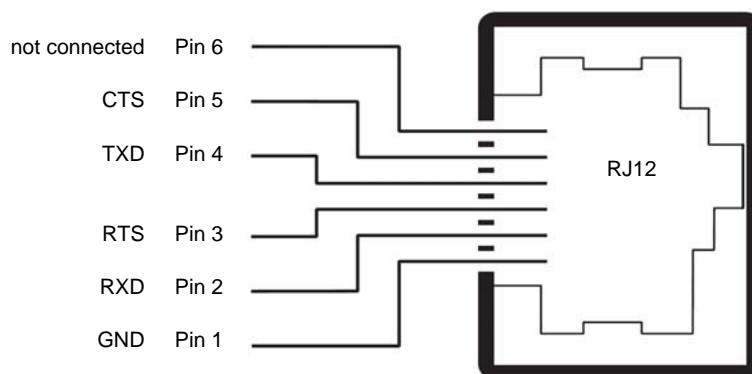
A PC is connected directly (over its serial interface) to the serial interface of the mGuard. The PC user can then use a terminal program to configure the mGuard via the command line interface.

Alternatively, a modem is connected to the serial interface of the mGuard.

This modem is connected to the telephone network (landline or GSM network). The user of a remote PC, which is also connected to the telephone network using a modem, can establish a PPP dial connection (PPP = Point-to-Point Protocol) to the mGuard, and can then configure it using their web browser.

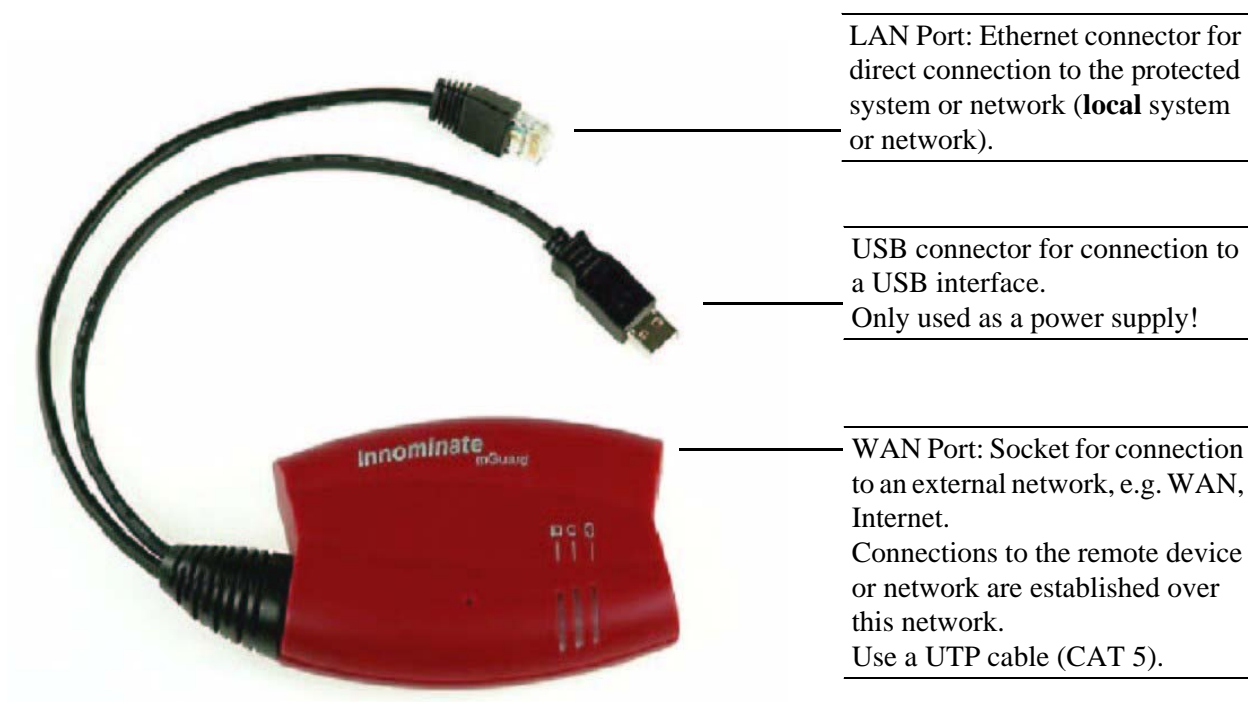
- b) For development of data transfers over the serial port instead of the mGuard WAN interface. In this case, a modem must be connected to the serial port.

### Pin assignment of the RJ12 jack (serial port)



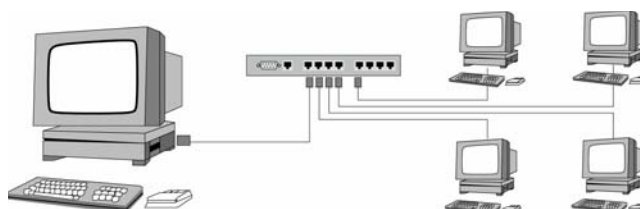
- ☒ Data traffic can pass over the *Analog line* or *ISDN line* instead of the WAN interface for the mGuard industrial RS with built-in modem or terminal adaptor.

## 4.2 Connecting the mGuard smart



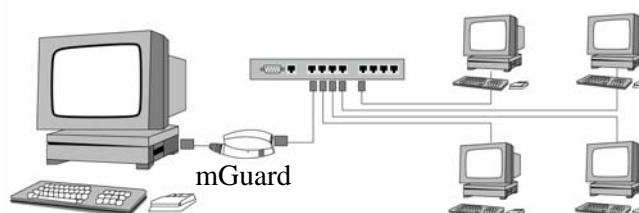
**If your computer is already attached to a network, then insert the mGuard between the existing network interface of the computer (network card) and the network.**

Before



After

(On the left side can also be a LAN.)



☒ Additional driver installation is not necessary.

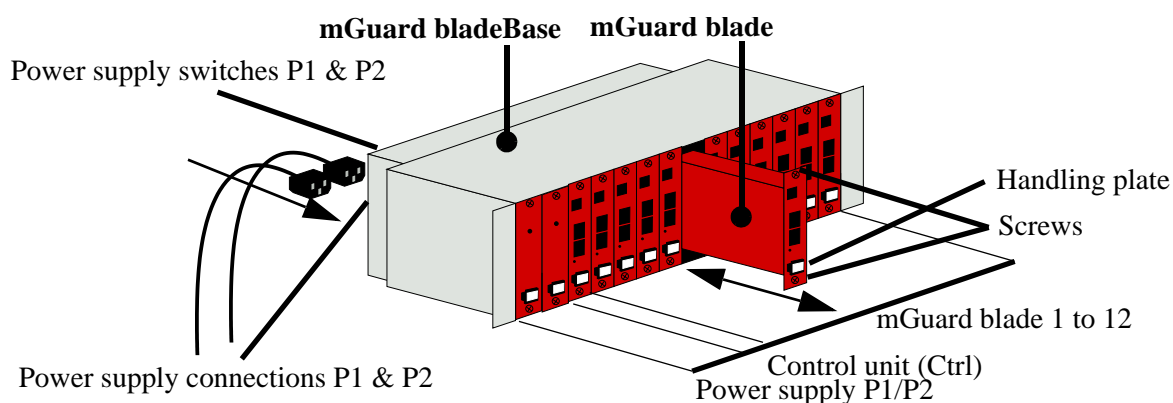
☒ For security reasons, we recommend that you change the default Root and Administrator passwords during the first configuration.

### Warning!



This is a Class A device, which may cause radio interference in residential areas, in which case the operator may be requested to take appropriate measures.

### 4.3 Installing the mGuard blade



#### Installing the mGuard bladeBase

- Install the mGuard bladeBase into the rack (e.g. close to the patch panel).
- Provide the two front power supplies and the control unit with the handling plates “P1”, “P2” and “Ctrl” from left to right.
- Connect both power supplies on the back of the mGuard bladeBase with 100V or 220/240V.
- Switch both power supplies on.
- The LEDs on the front of the power supplies should now light up green.

⊗ **It is very important to ensure sufficient air circulation for the bladePack!**

⊗ **When stacking several bladePacks, one or more rack mount fan trays must be installed to discharge the accumulated warm air!**

#### Installing the mGuard blade

- Loosen the upper and lower screw of the faceplate or mGuard blade to be replaced.
- Remove the faceplate or pull out the old mGuard blade.
- Insert the new mGuard blade and circuit board into the plastic guides and push until it is completely installed in the mGuard bladeBase.
- Secure the mGuard blade by tightening the screws lightly.
- Replace the empty handling plate with the suitable number from the mGuard bladeBase accessories or replace it with the plate of the old mGuard blade. To do this, pull or push in a sideways motion.
- ⊗ The mGuard bladeBase does not need to be switched off during installation or deinstallation of an mGuard blade.

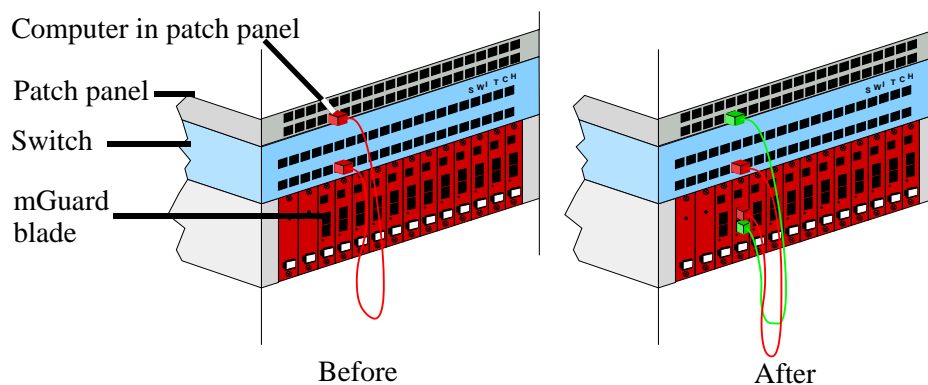
#### Control unit (CTRL slot)

The “CTRL” slot can be found directly next to both power supplies. An mGuard blade operated here works as a controller for all other mGuard blades.

During the first installation of an mGuard blade into the “CTRL” slot, the blade is reconfigured as a control unit as follows:

- The user interface is reconfigured for operation as a control unit.
- It switches into router mode with the local IP address 192.168.1.1.
- The firewall, anti-virus and VPN services are reset and deactivated.

## mGuard blade connection



If your computer is already attached to a network, then patch the mGuard blade between the existing network connection.

Please note that initial configuration can only be made from the local computer over the LAN interface. The mGuard firewall rejects all IP traffic from the WAN to the LAN interface.

☒ Additional driver installation is not necessary.

☒ For security reasons, we recommend that you change the default Root and Administrator passwords during the first configuration.

## Serial Port

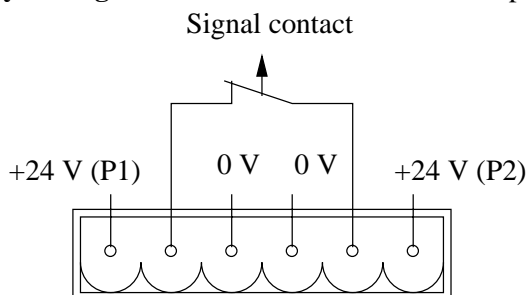


**Safety notice:** The serial interface (RJ12 jack) must not be connected directly to telephone lines. A serial cable with RJ12 plug has to be used to connect a serial terminal or a modem. The maximum length of the serial cable is 30m.

The serial port (serial interface) can be used the same way as described at “Serial Port” on page 29.

## 4.4 Installing the EAGLE mGuard

**Terminal block** The **power supply** and **signal contact** are connected via a 6 pin terminal block.



**! Safety notice:** The EAGLE mGuard is designed for operation with a safety extra-low voltage. Thus its power connections and signaling contact may only be connected to PELV circuits or alternatively SELV circuits with voltage restrictions in accordance with EN 60950-1.

The EAGLE mGuard can be operated using a direct current 9.6 - 60V DC max. 1A respectively an alternating current 18 - 30V AC max. 1A. Use the +24V and 0V pins to connect an alternating current.

### Operating voltage

NEC class 2 power source 12 V DC or 24 V DC -25% +33% safety extra-low voltage (SELV/PELV, decoupled redundant entries), max. 5 A. Buffer time min. 10 ms at 24 V DC.

### Redundant power supply

Redundant power supplies are supported. Both inputs are decoupled. There is no load distribution. With a redundant supply, only the power supply unit with the higher output voltage supplies the EAGLE mGuard. The supply voltage is electrically isolated from the housing.

### Signal contact

**! Safety notice:** The signaling contact may only be connected to PELV circuits or alternatively SELV circuits with voltage restrictions in accordance with EN 60950-1.

The signal contact is used to monitor the functions of the EAGLE mGuard and thereby allows remote diagnosis. The following is reported through interruption of the contact using potential-free signal contacts (relay contact, closed current circuit):

- The failure of at least one of the two supply voltages.
  - A permanent fault on the EAGLE mGuard (internal 3.3 V DC voltage, supply voltage 1 or 2 < 9.6 V, ...).
  - The faulty link status of at least one port. The link state report on the EAGLE mGuard can be masked on a port-by-port basis using the management software.
- No connection monitoring is offered in the supplied condition.

- Self-test error.

☒ In case of a non-redundant voltage supply, the EAGLE mGuard indicates the failure of the supply voltage. You can prevent this message by connecting the supply voltage to both inputs.

### Grounding connection

The EAGLE mGuard is grounded with a separate screw connection.

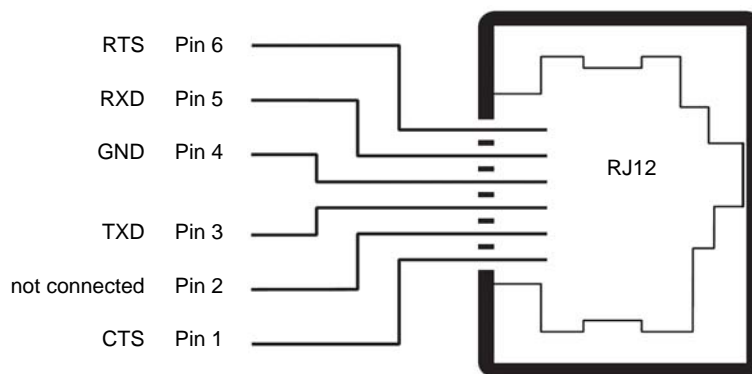
## Serial Port



**Safety notice:** The serial interface (RJ12 jack) must not be connected directly to telephone lines. A serial cable with RJ12 plug has to be used to connect a serial terminal or a modem. The maximum length of the serial cable is 30m.

The serial port (serial interface) can be used the same way as described at “Serial Port” on page 29. But the wiring of the serial port has to be different as shown with the following figure:

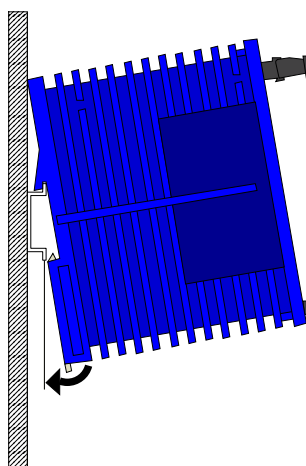
Pin assignment of the RJ12 jack (serial port)



## Assembly

The device is delivered in a ready-to-operate condition. The following procedure is required for the assembly process:

- Detach the terminal block from the EAGLE mGuard and connect the supply voltage and signal contact lines.
- Attach the EAGLE mGuard onto a 35 mm DIN rail according to DIN EN 50 022.
- Attach the upper snap-on guide of the EAGLE mGuard to the DIN rail and press it down until it locks into position.
- Connect the device to the local network or the local computer which is to be protected (LAN).
- Connect the socket for connection to the external network (WAN), for example, to the Internet. Connections to the remote device or network are established over this network.



- ☒ The front faceplate of the EAGLE mGuard housing is grounded via the grounding connection.
- ☒ Do not open the housing.
- ☒ The shielding ground of the connectable twisted pair lines is electrically connected to the front faceplate.

**Warning!**

This is a Class A device, which may cause radio interference in residential areas, in which case the operator may be requested to take appropriate measures. If installed in a living area or office environment, the EAGLE mGuard must be operated exclusively in switch cabinets with fire protection characteristics in accordance with EN 60950-1.

**Startup**

Start the EAGLE mGuard by connecting the supply voltage via the 6 pin terminal block. Lock the terminal block with the locking screw at the side.

**Network connection**

If your computer is already attached to a network, then patch the EAGLE mGuard *between* the existing network connection.

Please note that initial configuration can only be made over the LAN interface. The EAGLE mGuard firewall rejects all IP traffic from the WAN to the LAN interface.

☒ Additional driver installation is not necessary.

☒ For security reasons, we recommend that you change the default Root and Administrator passwords during the first configuration.

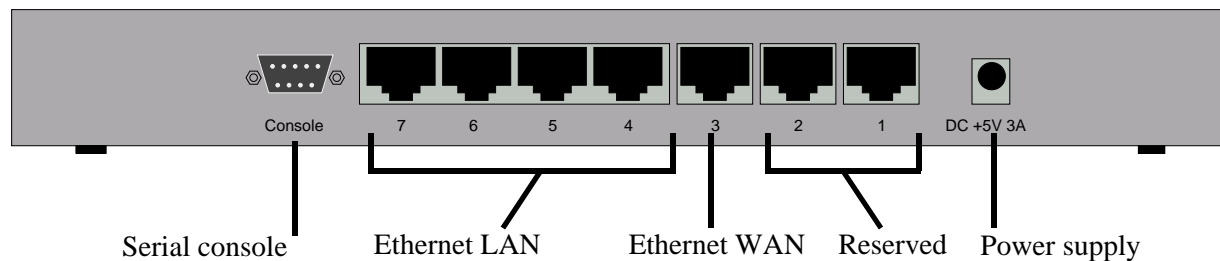
☒ Both network interfaces of the EAGLE mGuard are configured for connection to a computer. Please note the following when connecting to a hub: When *Automatic Negotiation* is deactivated, the Auto MDIX function is also deactivated. This means that the EAGLE mGuard port must be either connected to the uplink port of the hub or be connected using a cross-link cable.

**Disassembly**

To remove the EAGLE mGuard from the DIN rail, insert a screwdriver horizontally under the housing into the locking slide, pull it (without tipping the screwdriver) downwards and lift the EAGLE mGuard upwards.

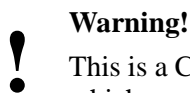
## 4.5 Connecting the mGuard delta

- ! **Safety notice:** The serial port (DE-9 connector) must not be connected directly to communication connection points. Use a serial cable with a DE-9 connector to connect a serial terminal or modem. The serial cable can have a maximum length of 30m.



- Connect the power supply (5 V DC, 3 A) to the corresponding mGuard power socket.
- Connect the local computer or network to one of the ethernet LAN sockets (4 to 7) using a UTP (CAT5) ethernet cable.

## 4.6 Installing the mGuard PCI



### Warning!

This is a Class A device, which may cause radio interference in a living area, in which case the operator may be requested to take appropriate measures.

### 4.6.1 Selection of Driver mode or Power-over-PCI mode

There are two operating modes: *Driver mode* or *Power-over-PCI mode*.

The mGuard is switched to the desired mode via a jumper.

#### Driver mode:

The mGuard PCI can be used like a normal network card. The network card then also provides the mGuard functions. In this case, the driver provided must be installed.

#### Power-over-PCI mode:

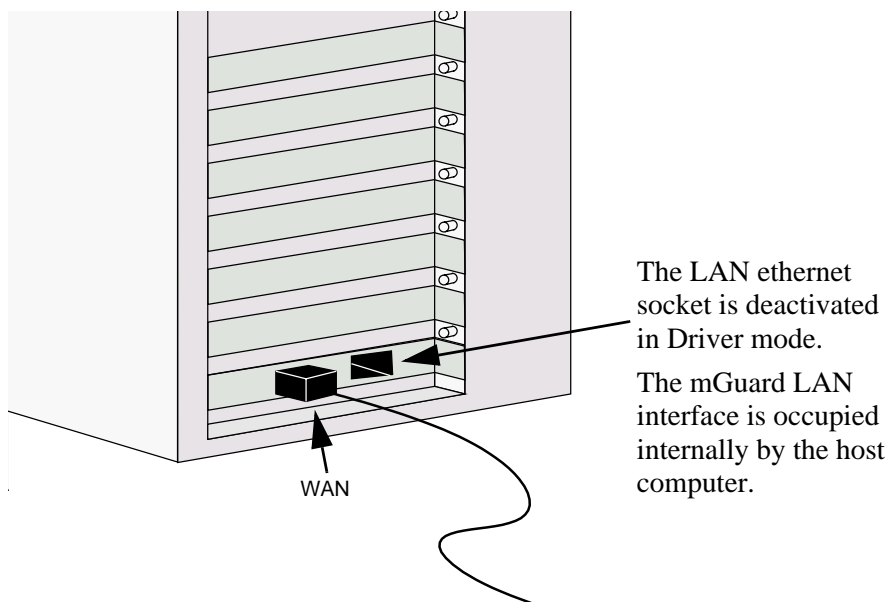
If the mGuard network card function is not needed or should not be used, then the mGuard PCI can be connected behind an existing network card (of the same or another computer). It then essentially acts as a stand-alone mGuard device. In reality, the mGuard PCI is only plugged into the PCI slot of the computer to receive a power supply and housing. This operating mode is known as *Power-over-PCI mode*. No drivers are installed.

Decide which mode the mGuard PCI should use before installation on your computer.

#### Driver mode

In this mode a mGuard PCI interface driver needs to be installed afterwards on the computer (available for Windows XP/2000 and Linux). No further network cards are required for the computer in Driver mode.

#### Stealth mode in Driver mode (factory default)

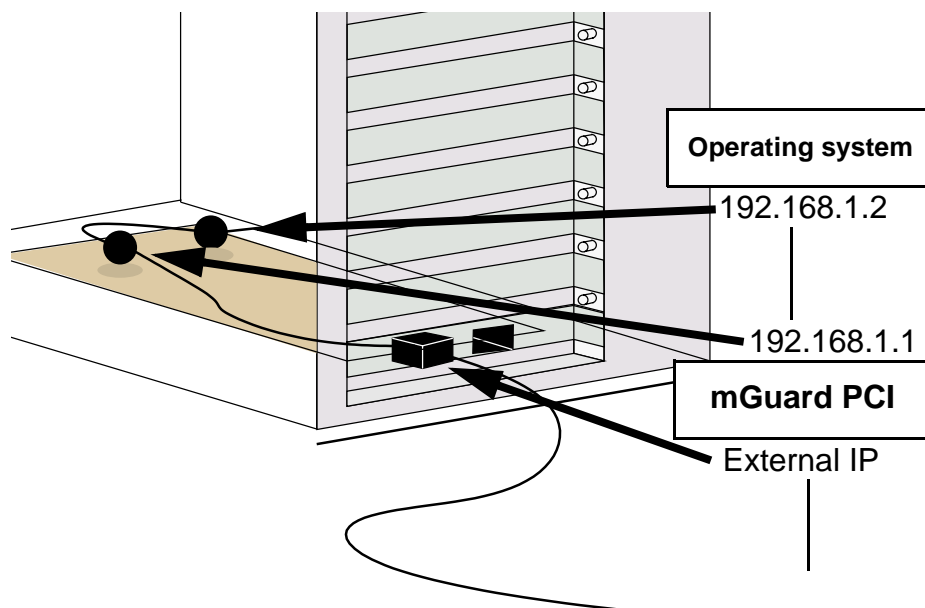


The mGuard in *Stealth* mode acts as a normal network card.

The IP address configured for the network interface of the operating system (LAN port) is also used by the mGuard for its WAN port. By doing this, the mGuard does not appear as an individual device with address for data traffic to and from the computer.

☒ It is not possible to use PPPoE or PPTP in Stealth mode.

### Router mode in Driver mode



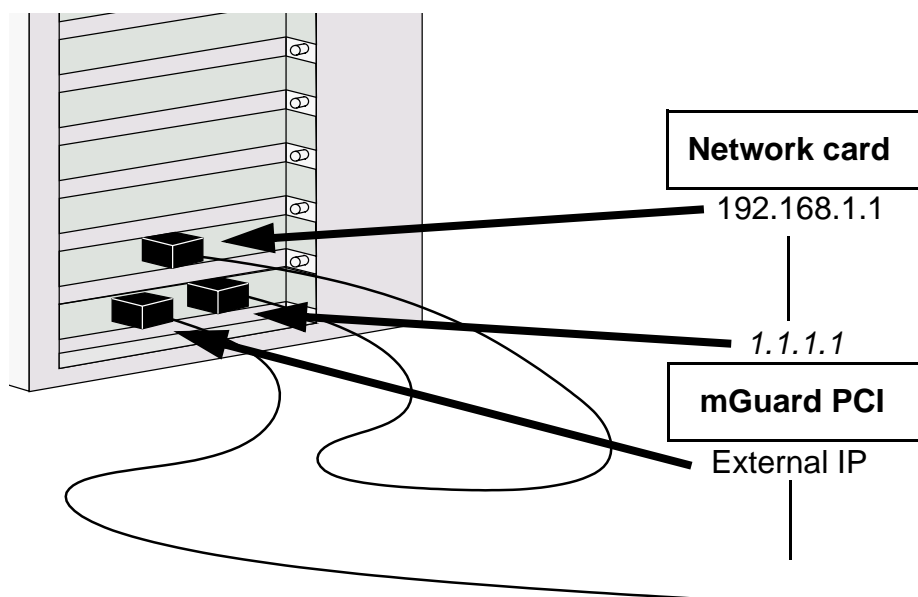
If the mGuard is in *Router* mode (or *PPPoE* or *PPTP* mode), then it builds its own network together with the operating system on the computer where the mGuard is installed. This means the following for the IP configuration of the operating system network interface: It must be assigned an IP address that is different to the IP address of the mGuard (according to the factory default of 192.168.1.1).

This is represented in the figure above by two black spheres.

A third IP is used for the mGuard interface to the WAN. Connection to an external network (e.g. Internet) is made using this IP.

### Power-over-PCI mode

#### Stealth mode in Power-over-PCI mode



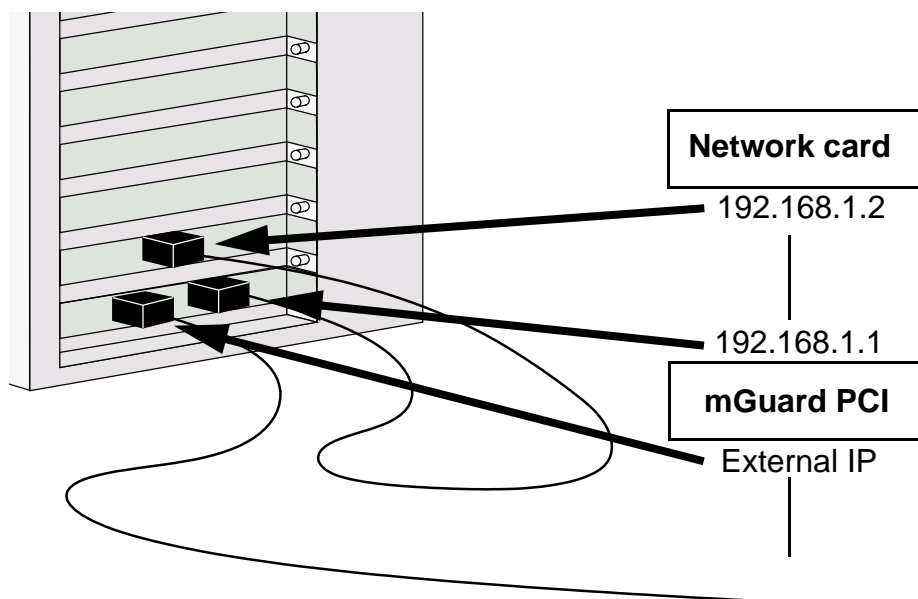
No driver software is installed in Power-over-PCI mode, as the mGuard PCI network card function is switched off.

A network card is connected to the LAN port of the mGuard PCI that is already installed and can be found on the same (or another) computer. (See “Hardware installation” on page 40.)

In *Stealth* mode, the IP address configured for the network interface of the operating system (LAN port) is also used by the mGuard for its WAN port. By doing this, the mGuard does not appear as an individual device with address for data traffic to and from the computer.

☒ It is not possible to use PPPoE or PPTP in Stealth mode.

### Router mode in Power-over-PCI mode

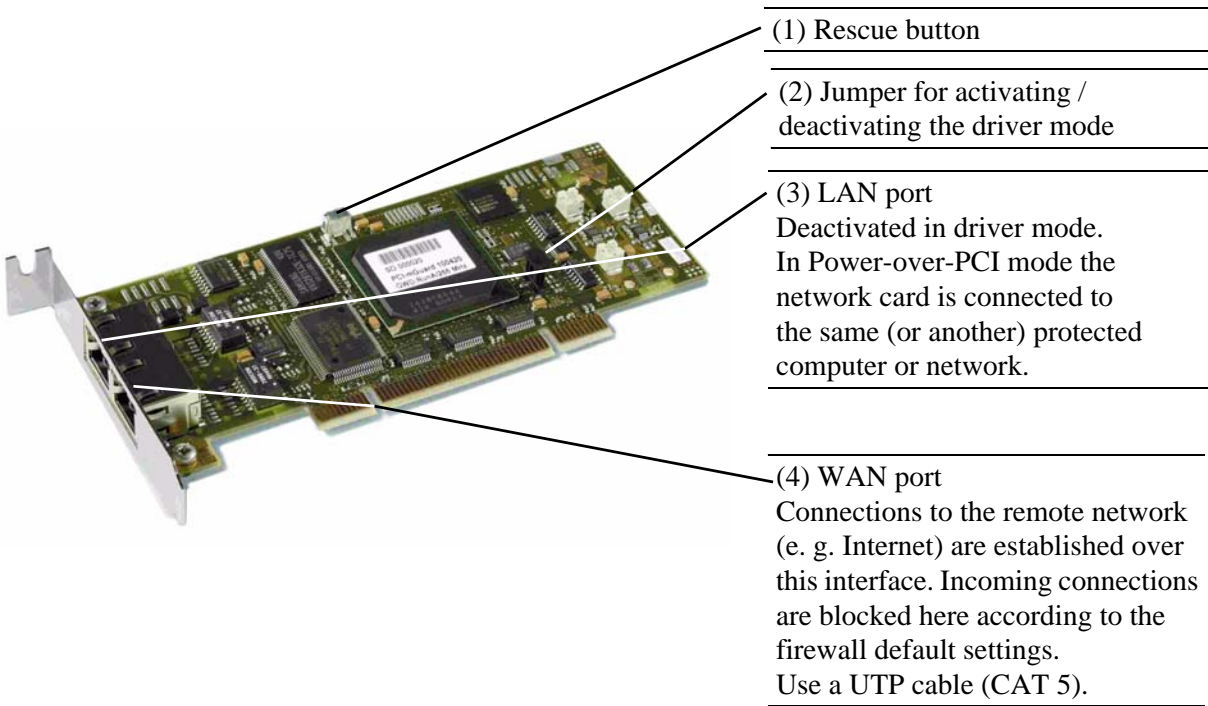


If the mGuard is in *Router* mode (or *PPPoE* or *PPTP* mode), then the mGuard and the network card connected to its LAN socket (either in the same or different computers) function as an individual network.

This means the following for the IP configuration of the network interface on the computer operating system: This network interface must be assigned an IP address that is different to the IP address of the mGuard (according to the factory default of 192.168.1.1).

A third IP is used for the mGuard interface to the WAN. Connection to an external network (e.g. Internet) is made using this IP.

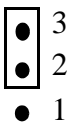
# 4.6.2 Hardware installation



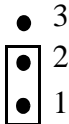
**Warning!**  
Before handling the mGuard PCI, touch the bare metal case of your PC to discharge the build-up of static electricity.

1. Configure the mGuard for *Driver mode* or *Power-over-PCI mode* (See “Selection of Driver mode or Power-over-PCI mode” on page 37.)  
To enable the required mode, set the jumper (2) to the following positions:

## Driver mode




## Power-over-PCI mode




2. Turn off the power to the computer and any other connected peripheral devices. Follow the precautions for the discharge of static electricity.
3. Unplug the power cable.
4. Open the computer cover. Please consult your computer manual.
5. Select a free PCI slot (3.3 V or 5 V) for the mGuard PCI.
6. Remove the relevant slot plate by loosening the holding screw and pulling it out. Keep this screw safe for securing the mGuard PCI card after installation.
7. Carefully align the connection plug board of the mGuard PCI card with the selected PCI slot on the motherboard, then push the card down evenly.
8. Tighten the card slot plate.
9. Close the computer cover.
10. Reconnect the power cable and turn on the computer.

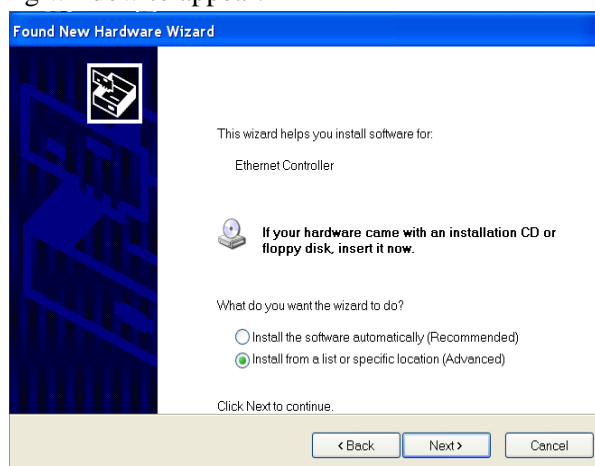
### 4.6.3 Driver installation

#### Windows XP

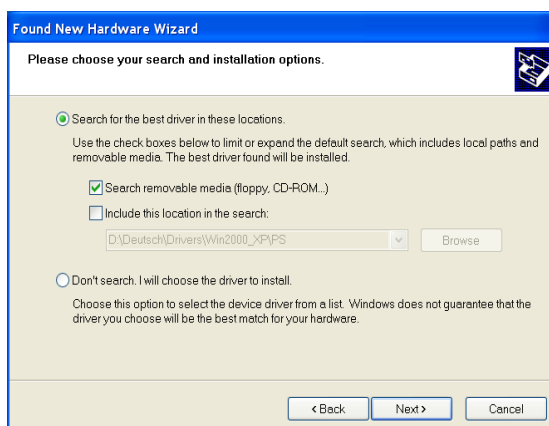
 Please first complete the steps described under “Hardware installation” on page 40.

 Installation of the driver is only necessary when the mGuard PCI operates in *Driver Mode* (see “Driver mode” on page 37).

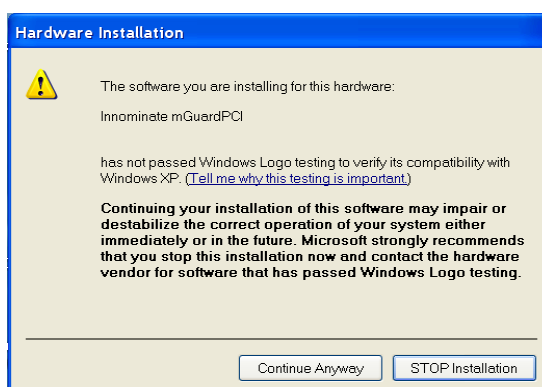
To install the driver, switch on the computer, login as an administrator and wait for the following window to appear:



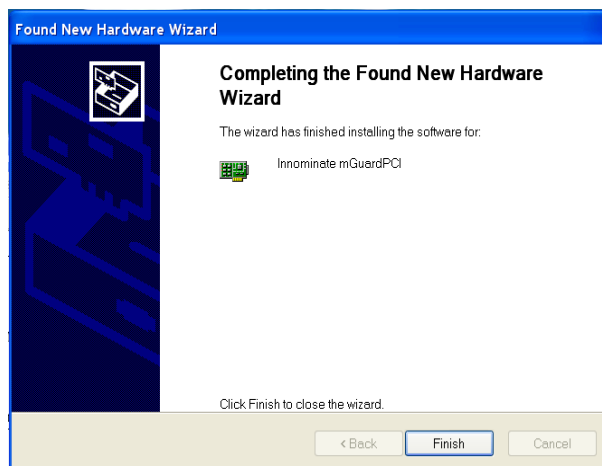
1. After inserting the mGuard CD choose the **Install from a list or specific location (Advanced)** option and click on **Next**.



2. Click on **Next**.



3. Click on **Continue Anyway**.



4. Click on **Finish**.

## Windows 2000



Please first complete the steps described under “Hardware installation” on page 40.

☒ Installation of the driver is only necessary when the mGuard PCI operates in driver mode (see “Driver mode” on page 37).

Switch on the computer, login and wait for the following window to appear:



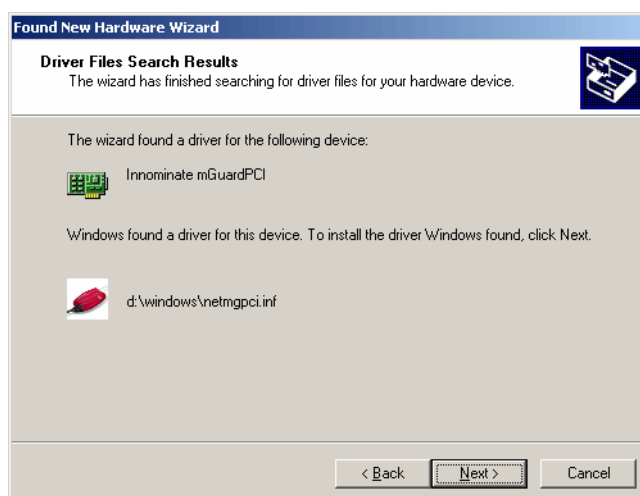
1. Click on **Next**.



2. After inserting the mGuard CD choose **Search for a suitable driver for my device** and click on **Next**.



3. Choose **CD-ROM drives** and click on **Next**.



4. Click on **Next**.



5. Click on **Yes**.



6. Click on **Finish**.

**Linux**

The Linux driver is available as a source archive and must be compiled before usage:

- Build and install the Linux kernel (2.4.25) in the **/usr/src/linux** directory
- Unpack the driver from the CD to **/usr/src/pci-driver**
- Enter the following commands:
  - **cd /usr/src/pci-driver**
  - **make LINUXDIR=/usr/src/linux**
  - **install -m0644 mguard.o /lib/modules/2.4.25/kernel/drivers/net/**
  - **depmod -a**
- The driver can then be loaded using the following command:
  - **modprobe mguard**

## 5 Preparing the configuration

### 5.1 Connection requirements

- |                             |  |
|-----------------------------|--|
| <b>mGuard industrial RS</b> | <ul style="list-style-type: none"><li>• The mGuard industrial RS must be connected to at least one active power supply.</li><li>• <u>For local configuration:</u> The computer used for configuration must be connected to the LAN socket of the mGuard.</li><li>• <u>For remote configuration:</u> The mGuard must be configured to permit remote configuration.</li><li>• The mGuard must be connected (i.e. the required connections must work).</li></ul>  |
| <b>mGuard smart</b>         | <ul style="list-style-type: none"><li>• The mGuard must be connected to a power supply (i.e. connected to an active system or power supply via USB cable).</li><li>• <u>For local configuration:</u> The computer used for configuration must either be<ul style="list-style-type: none"><li>– connected to the LAN port of the mGuard</li><li>– or connected to the mGuard via the local network.</li></ul></li><li>• <u>For remote configuration:</u> The mGuard must be configured to permit remote configuration.</li><li>• The mGuard must be connected (i.e. the required connections must work).</li></ul>  |
| <b>mGuard PCI</b>           | <ul style="list-style-type: none"><li>• <u>For local configuration:</u> The computer used for configuration must fulfill the following requirements:<ul style="list-style-type: none"><li>• <b>mGuard in <i>Driver mode</i>:</b> The mGuard PCI driver must be installed on the computer.</li><li>• <b>mGuard in <i>Power-over-PCI mode</i>:</b> The computer must be connected to the mGuard LAN port or connected to the mGuard over the local network.</li></ul></li><li>• <u>For remote configuration:</u> The mGuard must be configured to permit remote configuration.</li><li>• The mGuard must be connected (i.e. the required connections must work).</li></ul> |
| <b>mGuard blade</b>         | <ul style="list-style-type: none"><li>• The mGuard blade must be installed inside the mGuard bladeBase, and at least one of the bladeBase power supplies must be on.</li><li>• <u>For local configuration:</u> The computer used for configuration must either be<ul style="list-style-type: none"><li>– connected to the LAN socket of the mGuard</li><li>– or connected to the mGuard via the local network.</li></ul></li><li>• <u>For remote configuration:</u> The mGuard must be configured to permit remote configuration.</li><li>• The mGuard must be connected (i.e. the required connections must work).</li></ul>  |
| <b>EAGLE mGuard</b>         | <ul style="list-style-type: none"><li>• The EAGLE mGuard must be connected to at least one active power supply.</li><li>• <u>For local configuration:</u> The computer used for configuration must either be<ul style="list-style-type: none"><li>– connected to the LAN socket of the mGuard</li><li>– or connected to the mGuard via the local network.</li></ul></li><li>• <u>For remote configuration:</u> The mGuard must be configured to permit remote configuration.</li><li>• The mGuard must be connected (i.e. the required connections must work).</li></ul>   |
| <b>mGuard delta</b>         | <ul style="list-style-type: none"><li>• The mGuard must be connected to its power supply.</li><li>• <u>For local configuration:</u> The computer used for configuration must either be<ul style="list-style-type: none"><li>– connected to the mGuard LAN switch (ethernet socket 4 to 7)</li><li>– or connected to the mGuard via the local network.</li></ul></li><li>• <u>For remote configuration:</u> The mGuard must be configured to permit remote configuration.</li><li>• The mGuard must be connected (i.e. the required connections must work).</li></ul>   |

## 5.2 Local configuration: At startup

The mGuard is configured using the web browser running on the configuration system (e.g. Firefox (from version 1.5), MS Internet Explorer (from version 5.0) or Safari).

✉ **The web browser must support SSL (i.e. https).**

According to the factory defaults, the mGuard is accessible under the following address:

### Factory default:

Stealth mode: (Factory default settings, apart from mGuard delta and blade controller)	https://1.1.1.1/
Router mode: (Factory default for mGuard delta and blade controller)	https://192.168.1.1/

### 5.2.1 mGuard industrial RS, mGuard smart, mGuard blade and EAGLE mGuard

#### With a configured network interface

In order to access the mGuard via the address https://1.1.1.1/, it must be connected to a configured network interface. This is the case if it is inserted into an existing network connection – see the illustrations in the following sections:

- “Connecting the mGuard smart” on page 30

In this case, the web browser can establish a connection to the mGuard configuration interface after entering the address as https://1.1.1.1/ – see “Setting up a local configuration connection” on page 52. Continue from this point.

#### With a non-configured network interface

##### If the computer’s network interface has not been configured

If the configuration system was not previously connected to a network (e.g. because the computer is new), then the network interface is not usually configured. This means that the computer does not yet “know” that network traffic is handled by this interface.

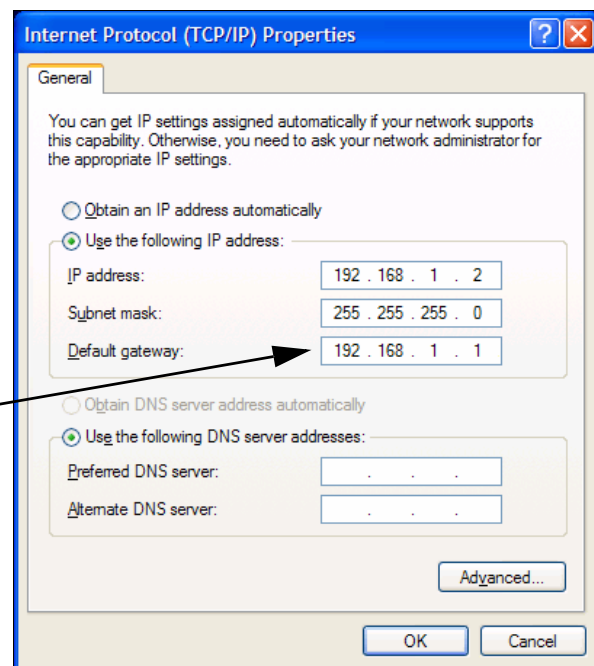
In this case, you must initialize the default gateway by assigning it a dummy value. To do this, proceed as follows:

##### Initializing the default gateway

1. Determine the currently valid default gateway address. If you are using Windows XP:
  - Click on **Start, Control Panel, Network Connections**.
  - Right click on the icon of the LAN adapter so that the pop-up menu appears. Click on **Properties**.
  - In the **Properties of LAN connections** local network on the *General* tab, select *Internet Protocol (TCP/IP)* under “This connection uses the

following items”. Then click on **Properties**, so that the following window is displayed:

The IP address of the default gateway can be searched for or set here



If no IP address has been entered as the default gateway in this text field (e.g. because the *Obtain an IP address automatically* function has been activated), then enter the IP address manually. To do so, first select **Use the following IP** and then enter the following addresses (example):

IP address:	192.168.1.2
Sub-netmask:	255.255.255.0
Default gateway:	192.168.1.1

☒ Do not under any circumstances assign an address like 1.1.1.2 to the configuration system!

- On the DOS level (**Start, Programs, Accessories, Command Prompt**), enter the following command:

**arp -s <IP of the default gateway> 00-aa-aa-aa-aa-aa**

Example:

You have determined or set the address of the default gateway as 192.168.1.1  
The command should then be:

**arp -s 192.168.1.1 00-aa-aa-aa-aa-aa**

- To proceed with the configuration, establish the necessary configuration connection – see “Setting up a local configuration connection” on page 52.
- After setting the configuration, restore the original setting for the default gateway address. To do this, either restart the configuration computer or enter the following command on the DOS level:

**arp -d**

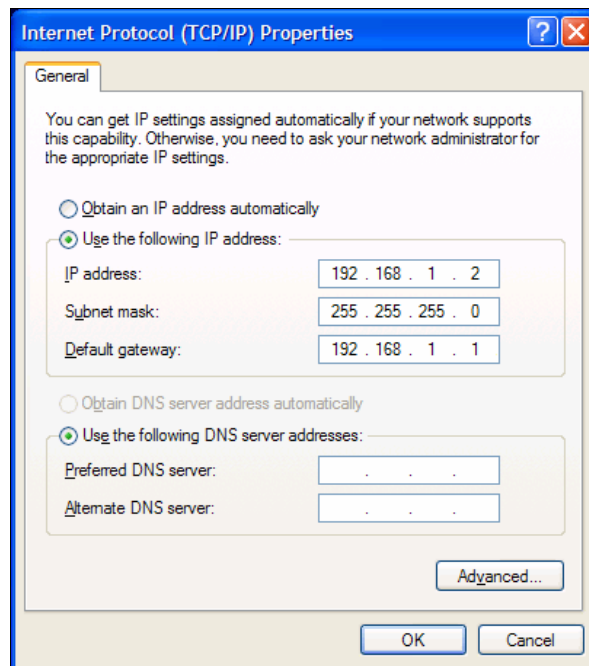
- ☒ Depending on the configuration of the mGuard, it may then be necessary to change the network interface of the local computer accordingly.

## 5.2.2 mGuard delta

After initial delivery, resetting to the factory defaults or flashing the mGuard, the mGuard delta is found on the LAN interfaces 4 to 7 under the address 192.168.1.1 within the network 192.168.1.0/24. You may need to adjust the configuration of your computer to access the necessary interface.

If you are using Windows XP:

- Click on **Start, Control Panel, Network Connections**.
- Right click on the icon of the LAN adapter so that the pop-up menu appears. Click on **Properties**.
- In the **Properties of LAN connections** local network on the *General* tab, select *Internet Protocol (TCP/IP)* under “This connection uses the following items”. Then click on **Properties**, so that the following window is displayed:



First select **Use the following IP** and then enter the following addresses (example):

IP address:	192.168.1.2
Sub-netmask:	255.255.255.0
Default gateway:	192.168.1.1

- ⊠ Depending on the configuration of the mGuard, it may then be necessary to change the network interface of the local computer accordingly.

### 5.2.3 mGuard PCI

#### Installing the PCI card

If the PCI card has not yet been installed in your computer, please first follow the steps as described in “Hardware installation” on page 40.

#### Installing the driver

If you have configured the mGuard to run in **Driver mode**, ensure that the drivers are installed as described under “Driver installation” on page 41.

#### Configuring the network interface

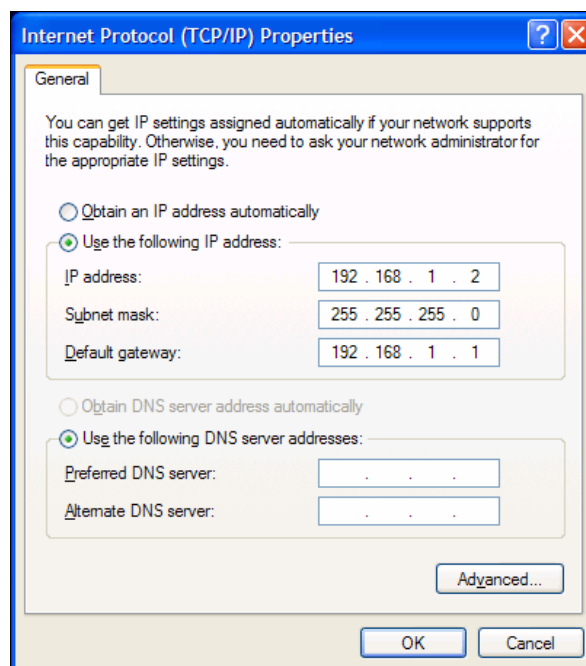
If you operate the mGuard

- in **Driver mode**, and the LAN interface has not yet been configured (i.e. network interface of the computer)
- OR

- in **Power-over-PCI mode** and the network interface of the computer connected to mGuard LAN interface has not yet been configured, then this network interface must be configured before you can configure mGuard.

If you are using Windows XP:

- Click on **Start, Control Panel, Network Connections**.
- Right click on the icon of the LAN adapter so that the pop-up menu appears. Click on **Properties**.
- In the **Properties of LAN connections** local network on the *General* tab, select *Internet Protocol (TCP/IP)* under “This connection uses the following items”. Then click on **Properties**, so that the following window is displayed:



#### Default gateway

After you have configured the network interface, you can access the mGuard configuration interface using a web browser under the URL “https://1.1.1.1/”. If this is not possible, then the default gateway of the computer may not be available. In this case you must simulate the process as follows:

#### Initializing the default gateway

1. Determine the currently valid default gateway address.

If you are using Windows XP, follow the steps described above (under “Configuring the network interface” on page 50) to open the **Internet Protocol (TCP/IP) Properties** text field.

If no IP address has been entered as the default gateway in this dialog box (e.g. because the *Obtain an IP address automatically* function has been activated),

then enter the IP address manually. To do so, first select **Use the following IP** and then enter the following addresses (example):

IP address:	192.168.1.2	<input checked="" type="checkbox"/> Do not under any circumstances assign an address like 1.1.1.2 to the configuration system!
Sub-netmask:	255.255.255.0	
Default gateway:	192.168.1.1	

---

2. On the DOS level (**Start, Programs, Accessories, Command Prompt**), enter the following command:

**arp -s <IP of the default gateway> 00-aa-aa-aa-aa-aa**

Example:

You have determined or set the address of the default gateway as 192.168.1.1

The command should then be:

**arp -s 192.168.1.1 00-aa-aa-aa-aa-aa**

---

3. To proceed with the configuration, establish the necessary configuration connection – see “Setting up a local configuration connection” on page 52.
- 

4. After setting the configuration, restore the original setting for the default gateway address. To do this, either restart the configuration computer or enter the following command on the DOS level:

**arp -d**

- ☒ Depending on the configuration of the mGuard, it may then be necessary to change the network interface of the local computer accordingly.

### 5.3 Setting up a local configuration connection

**Web-based administrator interface**

The mGuard is configured using the web browser running on the configuration system (e.g. Firefox, MS Internet Explorer or Safari).

☒ **The web browser must support SSL (i.e. https).**

Depending on the model, the mGuard is delivered either in *Stealth* or *Router* mode and is therefore available under one of the following addresses:

**Factory default:**

Stealth mode: (Factory default settings, apart from mGuard delta and blade controller)	https://1.1.1.1/
Router mode: (factory default for mGuard delta and blade controller)	https://192.168.1.1/

Proceed as follows:

1. Start the web browser.  
(e.g. Firefox, MS Internet Explorer or Safari; the web browser must support SSL (i.e. https)).
2. Ensure that the browser does not automatically dial a connection at startup, as this could make it more difficult to establish a connection to the mGuard. In MS Internet Explorer, make this setting as follows: In the **Extras** menu, select Internet Options... and click on the *Connections* tab: Ensure that **Never dial a connection** is selected under *Dial-up and Virtual Private Network settings*.
3. Enter the complete address of the mGuard in the address field of the browser. In **Stealth** mode (factory default except mGuard delta and blade controller), this is always

mGuard IP address in *Stealth* mode:  
**https://1.1.1.1/**

When not in *Stealth* mode:  
**https://192.168.1.1/**



**https://1.1.1.1/**

In **Router**, (factory default for mGuard delta and blade controller), PPPoE or **PPTP** mode this is always:

**https://192.168.1.1/**

Result:

You reach the mGuard administrator website. The security notice shown on the next page is displayed.

☒ If you have forgotten the configured address

If the address of the mGuard (in *Router*, *PPPoE* or *PPTP* mode) has been changed and the current address is unknown, you must use the **Recovery** key to set the mGuard to Stealth mode (or Router mode for mGuard delta and blade controller). This results in the resetting of the mGuard IP address factory defaults (see “Performing a recovery” on page 248).

☒ If the administrator website is not displayed

If the web browser repeatedly reports that the page cannot be displayed, try the following:

- Check whether the default gateway has been initialized on the connected configuration system. See “Local configuration: At startup” on page 47.
- Disable any active firewalls.
- Ensure that the browser does not use a proxy server.  
In MS Internet Explorer (version 6.0) make this setting as follows: In the **Extras** menu, select **Internet Options...** and click on the *Connections* tab: Under *LAN Settings* click on **Settings...** and check that **Use a proxy server for your LAN** (under proxy server) is not activated in the *Local Area Network (LAN) Settings*.
- If any other LAN connection is active on the system, deactivate it until configuration has been completed.  
Under the Windows menu **Start, Settings, Control Panel, Network Connections** or **Network and Dial-up Connections**, right click on the associated icon and select **Disable** in the pop-up menu.

### After a successful connection setup

After a connection has been successfully set up, the following security notice is displayed (MS Internet Explorer):



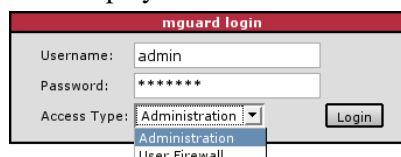
Explanation:

As administrative tasks can only be performed when secure (encrypted) access to the device has been established, a self-signed certificate is returned.

Acknowledge the associated security notice by clicking on **Yes**.

Result:

The login window is displayed:



Choose the access type (Administration or User Firewall) and enter your username and password for this access type. For the user firewall, see “Network Security → User Firewall” on page 178.

The factory defaults for administration purposes are:

**Login:**            **admin**  
**Password:**      **mGuard**

☒ Pay attention to capitalization!

To configure the device, make the required changes on the individual pages of the mGuard website.

See “Configuration” on page 56.

☒ For security reasons, we recommend that you change the default Root and Administrator passwords during the first configuration – see “Authentication → Local Users” on page 146.

## 5.4 Remote configuration

### Requirement

The mGuard must be configured to permit remote configuration.

☒ Remote configuration is disabled by default.

To enable remote configuration, see the section „Management → Web Settings“, “Access” on page 73.

### Remote configuration

To configure the mGuard from a remote computer using the web interface, first establish a connection to the mGuard.

Proceed as follows:

1. Start the web browser on the remote computer (e.g. Firefox, MS Internet Explorer or Safari; the web browser must support SSL (i.e. https)).
2. Under address, enter the IP address where the mGuard is available externally over the Internet or WAN, together with the port number (if required).

#### Example:

If this mGuard is accessible over the Internet at the address `https://123.45.67.89/` and the port number 443 has been set for remote access, then you need to enter the following address in the web browser on the remote peer: `https://123.45.67.89/`

If another port number is used then this is given behind the IP address, e. g.: `https://123.45.67.89:442/`

To configure the device, make the desired or necessary changes on the individual pages of the mGuard website.

See “Configuration” on page 56.

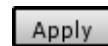
## 6 Configuration

### 6.1 Operation

#### Screen Layout

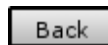
1. Click on the entry for the page with the desired setting possibilities on the left-hand menu, e.g. *Management* → *Licensing*. The page is then displayed in the main window as one or more pages, on which you can define the settings. If the page is organized into several pages, you can scroll through them using the *tabs* at the top.
2. Make the desired settings on the relevant page or tab. See also the section on “Working with sortable tables” on page 56.

3. Click on the **Apply** button to save the settings on the device.



After the settings have been saved by the system, you will see a confirmation message. This indicates that the new settings have taken effect. They also remain valid after a restart (reset).

- You can return to a previously accessed page by pressing the **Back** button, if available.



#### Entry of inadmissible values

After inadmissible values are entered (for example, an inadmissible number in an IP address) and after clicking on **Apply**, the relevant tab title is displayed in red. This helps in tracking down the error.

#### Working with sortable tables

Many settings are saved as data records. Accordingly, the adjustable parameters and their values are presented as table rows. If several data records have been set (e.g. firewall rules), these will be queried or processed based on the entry sequence from top to bottom. Therefore, pay attention to the order of the entries, if necessary. The sequence can be changed by moving table rows upwards or downwards.

With tables, you can carry out the following actions:

- Insert rows (sets up a new data record with settings (e.g. the firewall rules for a specific connection))
- Move rows (sorts them to another location)
- Delete rows (deletes the entire data record)

### Inserting rows

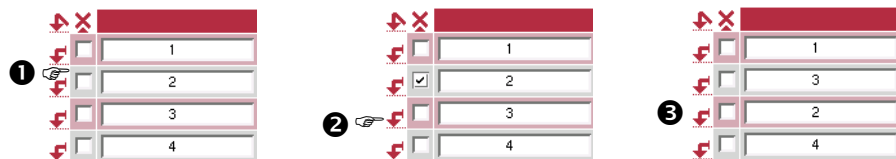


1. Click on the arrow where you want to insert a new row:



2. Result: The new row is inserted.  
You can now enter or specify values in the row.

### Moving rows

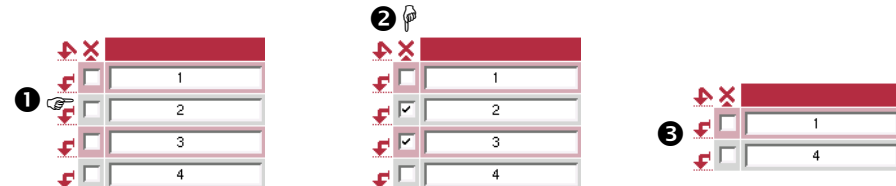


1. Select the row(s) you want to move.
2. Click on the arrow where you want to move the selected rows to:



3. Result: The rows are moved.

### Deleting rows



1. Select the rows you want to delete.
2. Click on the symbol to delete the rows:



3. Result: The rows are deleted.

### Working with non-sortable tables

Tables are non-sortable when the sequence of the data records contained within does not play any technical role. It is then not possible to insert or move rows. With such tables, you can carry out the following actions:

- Delete rows (as above under sortable tables).
- Append rows to the end of the table in order to create a new data record and settings (e.g. user firewall templates).

The symbols for appending and inserting a new table row are therefore different:



for appending rows to non-sortable tables



for inserting rows in sortable tables

### Appending rows (non-sortable tables)



1. Click on the arrow to insert a new row:



2. Result: The new row is appended under the existing table.  
You can now enter or specify values in the row.

### Further operating instructions

The following buttons are located at the top of every page:

	<p>Logout</p> <p>For logging out after configuration access to the mGuard. If the user does not conduct a logout procedure, the logout is automatically made when activities have stopped and the defined time limit has expired. Renewed access is only granted after the login process has been repeated.</p>
	<p>Reset</p> <p>Optional button. Resets data to the original values. If you have entered values on a configuration page and these have not yet been applied (<b>Apply</b> button), you can restore the original values on the page by clicking the <b>Reset</b> button. This button can only be seen at the top of the page if the validity range of the <b>Apply</b> button is set to <i>Include all pages</i> – see “Management → Web Settings” on page 72.</p>
	<p>Apply</p> <p>Optional button. Has similar functions to the <b>Apply</b> button but is valid for all pages. This button can only be seen at the top of the page if the validity range of the <b>Apply</b> button is set to <i>Include all pages</i> – see “Management → Web Settings” on page 72.</p>

## 6.2 Management Menu

- ☒ For security reasons, we recommend that you change the default Root and Administrator passwords during the first configuration – see “Authentication → Local Users” on page 146. You will be informed of this as long as passwords are left unchanged.

### 6.2.1 Management → System Settings

#### Host

Management » System Settings

Host

Signal Contact

Time and Date

☒ Shell Access

System

Power supply 1 / 2

failure / ok

Uptime

45 min

Temperature (°C)

0

45.0

60

System DNS Hostname

Hostname mode

User defined (from field below)

Hostname

machine01

Domain search path

beispiel-kunde-hh.com

SNMP Information

System Name

Location

Contact

HiDiscovery

Local HiDiscovery Support

Enabled

HiDiscovery Frame Forwarding

No

#### System (only mGuard industrial RS, EAGLE mGuard)

##### Power supply 1 / 2

State of both power supplies.

##### Uptime

Current system running time since the last reboot.

##### Temperature (°C)

An SNMP trap is sent if the temperature exceeds or falls below the defined temperature range.


#### System DNS Hostname

##### Hostname mode

You can assign a name to the mGuard using the *Hostname mode* and *Hostname* fields. For example, this is then displayed when logging in via SSH (see “Management → System Settings”, “Shell Access” on page 65). Assigning names simplifies the administration of several mGuards.

### **User defined (from field below)**

(Default) The name entered in the **Hostname** field is assigned to the mGuard.

 If the mGuard is running in *Stealth* mode, the option *User defined* must be selected under *Hostname mode*.

### **Provider defined (e.g. via DHCP)**

If the selected network mode permits external setting of the hostname (e.g. via DHCP), the mGuard is assigned the name received from the provider.

### **Hostname**

If the option *User defined* is selected under *Hostname mode*, enter the name that should be assigned to the mGuard here.

Otherwise, the entry in this field will be ignored (i.e. if the option *Provider defined (e.g. via DHCP)* is selected under *Hostname mode*).

### **Domain search path**

This option makes it easier for the user to specify a domain name. If the user enters the domain name in an abbreviated form, the mGuard completes the entry by appending the domain suffix that is defined here under the *Domain search path*.

## **SNMP Information**

### **System name**

A freely selectable name for the mGuard, used for administration purposes (e.g. “Hermes”, “Pluto”) (under SNMP: sysName).

### **Location**

Freely selectable description of the installation location (e.g. “hall IV”, “corridor 3”, “broom cupboard”) (under SNMP: sysLocation).

### **Contact**

The name of the contact person responsible for this mGuard, including telephone number (under SNMP: sysContact).

## **HiDiscovery**

HiDiscovery is a protocol which supports the initial startup of new network devices and is available in *Stealth* mode on the local interface (LAN) of the mGuard.

### **Local HiDiscovery Support**

#### **Enabled**

HiDiscovery protocol is activated.

#### **Read only**

HiDiscovery protocol is activated, but the mGuard cannot be configured using it.

#### **Disabled**

HiDiscovery protocol is deactivated.

### **HiDiscovery Frame Forwarding Yes / No**

If this option is set to **Yes**, then HiDiscovery frames are forwarded from the internal (LAN) port externally over the WAN port.

## Signal contact (only mGuard industrial RS, EAGLE mGuard)

The screenshot shows the 'Signal Contact' configuration window. It has a title bar 'Management >> System Settings' and four tabs: 'Host', 'Signal Contact' (selected), 'Time and Date', and 'Shell Access'. The 'Signal Contact' tab contains three sections: 'Mode' with a 'Signal contact' dropdown set to 'Operation supervision'; 'Operation supervision' with 'Contact' set to '[Open (Error)]', 'Redundant power supply' set to 'Supervise', and 'Link supervision' set to 'Ignore'; and 'Manual settings' with 'Contact' set to 'Closed'.

The signal contact is a relay which is used by the mGuard to signal error conditions (see also “Signal contact” on page 27 and Page 33).

### Mode

#### Signal contact

The signal contact can be controlled automatically by the mGuard using **Operation supervision** (default) or **Manual settings**.

See also:

“Installing the mGuard industrial RS” on page 24 and  
“Installing the EAGLE mGuard” on page 33.

### Operation supervision

#### Contact

Displays the state of the signal contact. Either **Open (Error)** or **Closed (OK)**.

#### Redundant power supply

If set to **Ignore**, the power supply does not influence the signal contact.  
If set to **Supervise**, the signal contact is opened if one of the two power supplies fails.

#### Link supervision

Supervision of the ethernet interface link state. Possible settings are:

- **Ignore**
- **Supervise internal only (trusted)**
- **Supervise external only (untrusted)**
- **Supervise both**

### Manual settings

#### Contact

If the **Signal contact** is set to **Manual setting** above, this option sets the contact to **Closed** or **Open (Alarm)**.

## Time and Date

### Time and Date

#### Current system time (UTC)

Displays the current system time in Universal Time Coordinates (UTC).

If *NTP time synchronization* is not yet activated (see below) and *Time stamp in filesystem* is deactivated, the clock will start at January 1st 2000.

#### Current system time (local)

Display: If you want the (sometimes different) current local time to be displayed, you must make the corresponding entry under *Timezone in POSIX.1 notation...* (see below).

#### Local system time

Display: Shows whether the system time and run time of the mGuard have ever actually been synchronized with a valid time. If the system time of the mGuard has not been synchronized, then the mGuard does not perform any time-controlled activities. These are as follows:

- Time-controlled pick-up of configuration from a configuration server:  
This is the case when the **Time Control** setting is selected under the *Management* → *Central Management*, *Get configuration* menu for the **Schedule** setting (see “6.2.5 Management → Configuration Profiles”, “Configuration Pull” on page 98).
- Interruption of the connection at a certain time using the PPPoE network mode:  
This is the case when PPPoE is set under the *Network* → *Interfaces*, *General* menu under **Network mode**. (see “6.4.1 Network → Interfaces”, “→ Network Mode: PPPoE” on page 120).
- Acceptance of certificates when the system time has not been synchronized:  
This is the case when the **Wait for system time synchronization** setting is selected under the *Authentication* → *Certificate*, *Certificate settings* menu for the **Check the validity period of certificates and CRLs** option (see “6.5.3 Authentication → Certificates”, “Certificate settings” on page 154).

The system time can be synchronized by various events:

- a) The mGuard possesses an installed clock which is synchronized with the current time at least once. The mGuard only has a clock when the **State of installed clock** option is visible. The display shows whether the clock is synchronized. A synchronized, installed clock ensures that the mGuard has a synchronized system time, even after rebooting.

- b) The administrator has defined the current time for the mGuard run time by entering the relevant values under **Local system time**.
- c) The administrator has set the **Timestamp in file system** to *Yes*, and has either transmitted the current system time to the mGuard by NTP (see below under *NTP server*) or under **Local system time**. The system time of the mGuard is then synchronized using the time stamp after rebooting (even if it has no installed clock and is set exactly again afterwards using NTP).
- d) The administrator has activated NTP time synchronization under **NTP Server**, has entered the address of at least one NTP server and the mGuard has opened connections with at least one of the defined NTP servers. If the network is working correctly then this occurs seconds after rebooting. The display in the **NTP state** field may only change to “synchronized” much later. See also the explanation below under **NTP state**.

### State of installed clock

(For *mGuard industrial RS* and *mGuard delta*)

The state of the installed clock is only visible when the mGuard possesses a clock that also runs when the system is turned off or has no power supply. The display shows if the clock has been synchronized with the current time. The installed clock is only synchronized when the system time of the mGuard is synchronized. If the clock has been synchronized then its status is only returned to “not synchronized” after the firmware is flashed.

### Local system time

Here you can set the mGuard time if no NTP server has been specified (see below) or the NTP server is not available.

The date and time are specified in the format YYYY.MM.DD-hh:mm:ss:

YYYY	Year
MM	Month
DD	Day
hh	Hour
mm	Minute
ss	Second

### Timezone in POSIX.1 notation...

If the *Current system time* above should display a current local time that is different to Greenwich Mean Time, then you must enter the number of hours that your local time is in front of or behind Greenwich Mean Time.

#### Example:

In Germany, the time is one hour after GMT. Therefore, enter: CET-1.

In New York the time is five hours behind Greenwich Mean Time. Therefore, enter: CET+5.

The only important thing is the -1, -2 or +1 value as only these are evaluated – not the preceding letters. They can be substituted with “CET” or any other designation, such as “UTC”.

If you wish to display Central European Time (e.g. for Germany) and have it automatically switch to/from daylight saving time, enter:

CET-1CEST,M3.5.0,M10.5.0/3

**Timestamp in filesystem (2h granularity): Yes / No**

If this option is set to **Yes**, the mGuard will save the current system time every two hours.

Result:

If the mGuard is switched off and then back on, a time from this two-hour time period is displayed, not a time on January 1, 2000.

**NTP Server**

(NTP - Network Time Protocol) The mGuard can obtain the current date and time from an NTP server (time server). In order to do this, the address of at least one NTP server must be entered. This feature must also be activated.

**Enable NTP time synchronization: Yes / No**

Once the NTP is enabled, the mGuard obtains the date and time from a time server and displays this as its current system time. Synchronization may take a few seconds.

**NTP State**

Displays the current NTP state.

Shows whether or not the NTP daemon installed in the mGuard has synchronized with the configured NTP server to a suitable level.

If the system clock of the mGuard has never been synchronized before activation of NTP time synchronization, then synchronization can take up to 15 minutes. The NTP daemon still changes the mGuard system clock to the current time as soon as it has successfully contacted an NTP server.

The system time of the mGuard is then synchronized.

Fine-adjustment of the time is usually only made in the second range.

**NTP Server**

Enter one or more time servers from which the mGuard should obtain the current time. If you enter several time servers, the mGuard will automatically connect with all of them to determine the current time.

☞ If you enter a hostname, e.g. pool.ntp.org, instead of an IP address, a valid DNS server must also be specified – see “Network → DNS” on page 139.

## Shell Access

Displayed when  
Enable X.509  
certificates for SSH  
access is set to Yes.

**Management > System Settings**

Host | Signal Contact | Time and Date | **Shell Access**

**Shell Access**

Session Timeout (seconds) 0

Enable SSH remote access No

Port for incoming SSH connections (remote administration only) 22

**Allowed Networks**

N°	From IP	Interface	Action	Comment	Log
1	0.0.0.0/0	External	Accept		No

**X.509 Authentication**

Enable X.509 certificates for SSH access Yes

SSH server certificate None

CA certificate

X.509 subject

Authorized for access as All users

Client certificate

Authorized for access as All users

These rules allow to enable SSH remote access.  
Important: Make sure to set secure passwords before enabling remote access.  
Note: In Stealth mode incoming traffic on the given port is no longer forwarded to the client.  
Note: In router mode with NAT or portforwarding the port set here has priority over portforwarding.  
Note: The SSH access from the internal side and via dial-in is enabled by default and can be restricted by firewall rules.

## Shell Access

When SSH remote access is enabled, the mGuard can be configured from a remote system using the command line interface.

This option is disabled by default.

**IMPORTANT:** If you enable remote access, ensure secure *root* and *administrator* passwords are defined.

To enable SSH remote access, make the following settings:

### Session Timeout (seconds)

Specifies after how long (in seconds) the session is automatically ended when no action is taken (i.e. automatic logout). The setting “0” (factory default) means that no automatic session end is made.

The given value is also valid for shell access over the serial port.

### Enable SSH remote access: Yes / No

If you want to enable SSH remote access, then set this option to **Yes**. You can enable *Internal* SSH access (i.e. from the directly connected LAN or from the directly connected computer) independently of the switch setting.

You must define the firewall rules for the available interfaces on this page under **Allowed networks** in order to specify access possibilities to the mGuard.

### Port for incoming SSH connections (remote administration only)

Standard: 22

If this port number is changed, the new port number only applies for access over the *External*, *External 2* and *VPN* interfaces and over *Dial-in*. Port number 22 still applies for internal access.

The remote peer that makes remote access may have to enter the port number defined here during the login procedure.

Example:

If this mGuard is accessible over the Internet under the address 123.124.125.21, and the standard port number 22 has been set for remote access, you may not need to enter this port number in the address field on the SSH client (e.g. PuTTY or OpenSSH) of the remote peer.

If a different port number has been set (e.g. 2222), this must be specified, e.g.:  
ssh -p 2222 123.124.125.21

## Allowed Networks

Allowed Networks

Log ID: fw-ssh-access-Nº-3e8b12d0-3d40-1fd9-97e6-000cbe0220cf

✕	✕	Nº	From IP	Interface	Action	Comment	Log
✕		1	10.1.0.0/16	External	Accept		No

Lists the firewall rules that have been set. These apply for incoming data packets of an SSH remote access attempt.

If multiple firewall rules are set, they will be searched in the order in which they are listed (top-down) until a suitable rule is found. This rule is then applied. If there are other suitable rules further down the list, then these are ignored.

- ☒ The rules specified here only become effective if **Enable SSH remote access** is set to **Yes**. *Internal* access is also possible when this option is set to **No**. A firewall rule that would refuse *Internal* access is therefore not effective in this case.

You have the following options:

### From IP

In this field you enter the address of the system or network where remote access is permitted or forbidden.

You have the following options:

- IP address: **0.0.0.0/0** means all addresses. To enter an address, use CIDR notation – see “CIDR (Classless Inter-Domain Routing)” on page 246.

### Interface

**External / Internal / External 2 / VPN / Dial-in<sup>1</sup>**

Specifies which interface the rules apply to.

If no rules are set, the following default settings apply:

SSH access is permitted over *Internal*, *VPN* and *Dial-in*. Access over *External* and *External 2* is refused.

If required, you can specify the access possibilities.

#### Caution:

If you want to refuse access over *Internal*, *VPN* or *Dial-in*, you must implement this explicitly through corresponding firewall rules, by specifying *Drop* as an action, for example. To avoid locking yourself out, you may have to simultaneously allow access over another interface explicitly with *Accept* before you make the new setting effective by clicking the **Apply** button. Otherwise, if you are locked out, you must perform the recovery procedure.

1. *External 2* and *Dial-in* only for devices with serial ports.  
See “Network → Interfaces” on page 105.

Action

Possible settings:

- Accept
- Reject
- Drop

**Accept** means that data packets may pass through.

**Reject** means that the data packets are rejected. The sender is informed that the data packets have been rejected. In *Stealth* mode, *Reject* has the same effect as *Drop*.

**Drop** means that data packets may not pass through. The data packets are discarded and the sender is not informed of their whereabouts.

Comment

Freely selectable comment for this rule.

Log

For each individual firewall rule you can specify whether the use of the rule

- should be logged (set *Log* to **Yes**) or
- should not be logged (set *Log* to **No** – factory default)

X.509 Authentication

Enable X.509 certificates for SSH access: Yes / No

If **No** is selected, then only normal authentication procedures (user name and password or private and public keys) are allowed, not the X.509 authentication procedure.

If **Yes** is selected then the X.509 authentication procedure can be used in addition to normal procedures (as seen under **No**).

When **Yes** is selected, the following points must be defined:

- a) How the local mGuard authenticates itself to the SSH client according to X.509
- b) How the local mGuard authenticates the remote SSH client according to X.509

X.509 Authentication

Enable X.509 certificates for SSH access	Yes
SSH server certificate	None

CA certificate

X.509 subject

Authorized for access as

All users

Client certificate

Authorized for access as

All users

These rules allow to enable SSH remote access.

Important: Make sure to set secure passwords before enabling remote access.

Note: In Stealth mode incoming traffic on the given port is no longer forwarded to the client.

Note: In router mode with NAT or portforwarding the port set here has priority over portforwarding.

Note: The SSH access from the internal side and via dial-in is enabled by default and can be restricted by firewall rules.

### → a) How the mGuard authenticates itself to the SSH client

#### SSH server certificate

Specifies how the mGuard identifies itself to the SSH client.

Select one of the machine certificates from the list or the *None* entry (see below).

*None*:

When *None* is selected, the SSH daemon of the mGuard does not authenticate itself to the SSH client via the X.509 certificate. Instead, it uses a server key and is thus compatible with older versions of the mGuard.

If one of the machine certificates is selected then this is also offered to the SSH client. The client can then decide whether to use the normal authentication procedure or the procedure according to X.509.

The selection list gives a selection of machine certificates that are loaded in the mGuard under the *Authentication → Certificate* menu – see “Authentication → Certificates” on page 150 of this manual.

### → b) How the mGuard authenticates the remote SSH client



The following definition relates to how the mGuard verifies the authentication of the remote SSH client.

The table below shows which certificates must be provided for the mGuard to authenticate the SSH client if the SSH client displays one of the following certificate types on connection:

- A certificate signed by a CA
- A self-signed certificate

For further information on the following table see chapter “6.5.3 Authentication → Certificates” on page 150.

#### Authentication for SSH

The remote peer shows the following:	Certificate (specific to individual) <b>signed by CA</b>	Certificate (specific to individual) <b>self-signed</b>
The mGuard authenticates the remote peer using:		
	<p>All CA certificates that build the chain to the root CA certificate together with the certificates displayed by the remote peer</p> <p>or ADDITIONALLY</p> <p>Remote certificates, <u>if</u> used as filter</p>	Remote certificate

According to this table, the certificates must be provided that the mGuard uses for authentication of the respective SSH client.

The following instructions assume that the certificates have been correctly installed in the mGuard. See “6.5.3 Authentication → Certificates” on page 150.

- ☒ If the use of block lists (CRL checking) is activated under the *Authentication → Certificate, Certificate settings* menu point, then each certificate signed by a CA that shows an SSH client is checked for blocks.

### CA certificate

The configuration is only necessary when the SSH client displays a certificate signed by a CA.

All CA certificates needed by the mGuard to build the chain to the respective root CA certificate with the certificates displayed by the SSH client must be configured.

The selection list shows the machine certificates that are loaded in the mGuard under the *Authentication → Certificate* menu.

### X.509 Subject

Allows setting of a filter relating to the contents of the *Subject* field in the certificate displayed by the SSH client. It is then possible to limit or grant access by SSH clients who would accept the mGuard in principle based on the certification check:

- Limitation to certain *subjects* (i.e. individuals) or to *subjects* that have certain attributes
- or
- Grant for all subjects

(See also glossary under “Subject, certificate”.)

The *X.509 subject* field must not be left empty.

#### **Grant for all subjects (individuals):**

With a \* in the *X.509 subject* field, you can define that all subject entries are allowed in the certificate displayed by the SSH client. Identification or definition of the subject in the certificate is then no longer needed.

#### **Limitation to certain subjects (individuals) or to subjects that have certain attributes:**

In the certificate, the certificate owner is entered in the *Subject* field. The entry is comprised of several attributes. These attributes are either expressed as an Object Identifier (e.g.: 132.3.7.32.1) or, more commonly, as an abbreviation with a relevant value.

Example: CN=John Smith, O=Smith and Co., C=UK

If certain subject attributes have very specific values for the acceptance of the SSH client by the mGuard, then these must be specified accordingly.

The values of the other freely selectable attributes are entered using the \* wildcard.

Example: CN=\*, O=\*, C=UK (with or without empty spaces between attributes)

In this example the attribute “(C=UK)” must be entered in the certificate under “subject”. Only then does the mGuard accept the certificate owner (subject) as a communication partner. The other attributes in the certificates to be filtered can have freely selectable values.

- ☞ If a subject filter is set, the number (but not the sequence) of the entered attributes must correspond to those of the certificates where the filter is to be used.  
Pay attention to capitalization.
- ☞ Several filters can be set, their order is irrelevant.

#### **Authorized for access as: All users / root / admin / netadmin / audit**

Additional filter which defines that the SSH client has to have certain administration level authentication in order to gain access.

Explanation:

During connection, the SSH client shows its certificate and also the system user for which the SSH session is to be opened (*root*, *admin*, *netadmin*, *audit*). Access is only granted when the entries match those defined here.

Access for all listed system users is possible when *All users* is set.

- ☞ The *netadmin* and *audit* settings relate to access rights with the Innominate Device Manager.

#### **Client certificate**

Configuration is required in the following cases:

- SSH clients each show a self-signed certificate.
- SSH clients each show a certificate signed by a CA. Filtering should take place: Access is only granted to the user whose certificate copy is installed in the mGuard as the remote certificate and is provided in the mGuard table as *Client certificate*.

This filter is not subordinate to the *Subject* filter. It resides on the same level and is allocated a logical OR function with the *Subject* filter.

The entry in this field defines which remote certificate the mGuard should adopt in order to authenticate the remote peer (SSH client).

To do this, select one of the remote certificates from the selection list.

The selection list gives a selection of remote certificates that are loaded in the mGuard under the *Authentication* → *Certificate* menu.

**Authorized for access as: All users / root / admin / netadmin / audit**

Filter which defines that the SSH client has to have certain administration level authentication in order to gain access.

Explanation:

During connection, the SSH client shows its certificate and also the system user for which the SSH session is to be opened (*root*, *admin*, *netadmin*, *audit*).

Access is only granted when the entries match those defined here.

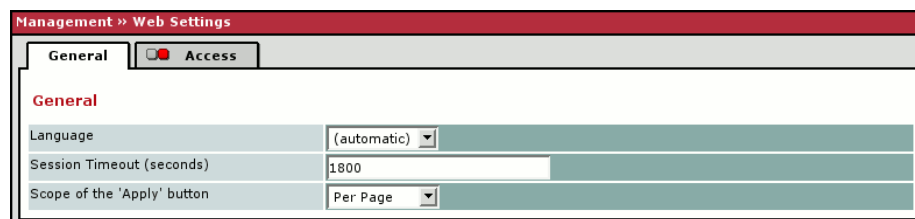
Access for all listed system users is possible when *All users* is set.



The *netadmin* and *audit* settings relate to access rights with the Innominate Device Manager.

## 6.2.2 Management → Web Settings

### General



Management >> Web Settings	
<b>General</b> <b>Access</b>	
<b>General</b>	
Language	(automatic) ▼
Session Timeout (seconds)	1800
Scope of the 'Apply' button	Per Page ▼

### General

#### Language

If **(automatic)** is selected from the list of languages, the device uses the language setting of the system browser.

#### Session Timeout (seconds)

Specifies the time interval of inactivity (in seconds) after which the user will be logged out automatically. Possible values: 15 to 86400 (= 24 hours)

#### Scope of the “Apply” button

The **Per Page** setting specifies that on every page on which you make changes you have to click the **Apply** button for the settings to be accepted and applied by the mGuard.

The **Per Session** setting specifies that you only have to click **Apply** once after making changes on a number of pages.

## Access

Only displayed  
during Login with  
X.509 user  
certificate

Management >> Web Settings

General Access

**HTTPS Web Access**

Enable HTTPS remote access No

Remote HTTPS TCP Port 443

**Allowed Networks**

No	From IP	Interface	Action	Comment	Log
1	0.0.0.0/0	External	Accept		No

**User authentication**

User authentication method Login with X.509 client certificate or password

**CA certificate**

**X.509 Subject**

**Authorized for access as**

**X.509 Certificate**

**Authorized for access as**

Log ID: fw-https-access-NP-00000000-0000-0000-0000-000000000000

These rules allow to enable HTTPS remote access.  
**Important: Make sure to set secure passwords before enabling remote access.**  
*Note:* In Stealth mode incoming traffic on the given port is no longer forwarded to the client.  
*Note:* In router mode with NAT or portforwarding the port set here has priority over portforwarding.  
*Note:* The HTTPS access from the internal side and via dial-in is enabled by default and can be restricted by firewall rules.

When web access by HTTPS protocol is enabled, the mGuard can be configured from a remote system using its web-based administrator interface. This means a browser running on the remote system is used to configure the local mGuard.

This option is disabled by default.

**IMPORTANT:** If you enable remote access, ensure secure *root* and *administrator* passwords are defined.

To enable HTTPS remote access, proceed as follows:

### HTTPS Web Access

#### Enable HTTPS remote access: Yes / No

If you want to enable HTTPS remote access, set this option to **Yes**. You can enable *Internal* HTTPS remote access (i.e. from the directly connected LAN or from the directly connected computer) independently of this switch setting.



You must define the firewall rules for the available interfaces on this page under **Allowed networks** in order to specify access possibilities to the mGuard.

Additionally, the authentication rules under **User authentication** must be set, if necessary.

#### Remote HTTPS TCP Port

Standard: 443

If this port number is changed, the new port number only applies for access over the *External*, *External 2* and *VPN* interfaces and over *Dial-in*.

Port number 443 still applies for internal access.

The remote peer that makes remote access must, if necessary, enter the port number defined here during entry of the address after the IP address.

Example:

If this mGuard is accessible over the Internet under the address 123.124.125.21 and the port number 443 has been set for remote access, then you do not need to enter this port number after the address in the web browser on the remote peer.

If another port number is used then this is given behind the IP address as follows : `https://123.124.125.21:442/`

NOTE:

- ☒ The mGuard authenticates itself to the remote peer using a self-signed machine certificate (in this case the browser of the user making remote access). This is a certificate produced once by Innominate for each mGuard. This means that each mGuard is delivered with an individual, self-signed machine certificate.

## Allowed Networks

Allowed Networks

Log ID: fw-https-access-Nº-3e8b12cf-3d40-1fd9-97e6-000cbe0220cf

Nº	From IP	Interface	Action	Comment	Log
1	0.0.0.0/0	External	Accept		No

Lists the firewall rules that have been set. These apply for incoming data packets of an HTTPS remote access attempt.

If multiple firewall rules are set, they will be searched in the order in which they are listed (top-down) until a suitable rule is found. This rule is then applied.

If there are other suitable rules further down the list, then these are ignored.

- ☒ The rules specified here only become effective if **Enable HTTPS remote access** is set to **Yes**. *Internal* access is also possible when this option is set to **No**. A firewall rule that would refuse *Internal* access is therefore not effective in this case.

You have the following options:

### From IP

In this field you enter the address of the system or network where remote access is permitted or forbidden.

- IP address: **0.0.0.0/0** means all addresses. To enter an address, use CIDR notation – see “CIDR (Classless Inter-Domain Routing)” on page 246.

### Interface

**External / Internal / External 2 / VPN / Dial-in<sup>1</sup>**

Specifies which interface the rules apply to.

If no rules are set, the following default settings apply:

HTTPS access is permitted over *Internal*, *VPN* and *Dial-in*. Access over *External* and *External 2* is refused.

If required, you can specify the access possibilities.

1. *External 2* and *Dial-in* only for devices with serial ports.  
See “Network → Interfaces” on page 105.

**Caution:**

If you want to refuse access over *Internal*, *VPN* or *Dial-in*, you must implement this explicitly through corresponding firewall rules, by specifying *Drop* as an action, for example. To avoid locking yourself out, you may have to simultaneously allow access over another interface explicitly with *Accept* before you make the new setting effective by clicking the **Apply** button. Otherwise, if you are locked out, you must perform the recovery procedure.

**Action**

Possible settings:

- Accept
- Reject
- Drop

**Accept** means that data packets may pass through.

**Reject** means that the data packets are rejected. The sender is informed that the data packets have been rejected. In *Stealth* mode, *Reject* has the same effect as *Drop*.

**Drop** means that data packets may not pass through. The data packets are discarded and the sender is not informed of their whereabouts.

**Comment**

Freely selectable comment for this rule.

**Log**

For each individual firewall rule you can specify whether the use of the rule

- should be logged (set *Log* to **Yes**) or
- should not be logged (set *Log* to **No** – factory default)

**User authentication**

**User authentication**

User authentication method Login with X.509 client certificate or password ▾

<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<b>CA certificate</b>	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="Web-RootCA 01"/>	▾
<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="Web-SubCA 01"/>	▾
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<b>X.509 Subject</b>	<b>Authorized for access as</b>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="*"/>	<input type="text" value="admin"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<b>X.509 Certificate</b>	<b>Authorized for access as</b>
<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="Meyer, Ralf"/>	<input type="text" value="admin"/>

These rules allow to enable HTTPS remote access.  
**Important: Make sure to set secure passwords before enabling remote access.**  
*Note:* In Stealth mode incoming traffic on the given port is no longer forwarded to the client.  
*Note:* In router mode with NAT or portforwarding the port set here has priority over portforwarding.  
*Note:* The HTTPS access from the internal side is enabled by default and can be restricted by firewall rules.

**User authentication method**

**Login with password**

Defines how the local mGuard authenticates the remote peer

Specifies that the remote mGuard user must use a password for authentication. The password is specified under the *Authentication* → *Local Users* menu. For more details, see “Authentication → Local Users” on page 146 of this manual.

Depending on which user ID is used (user or administrator password), the user has the right to operate and configure the mGuard.

**Login with X.509 client certificate or password**

Specifies the following:

1 User authentication is made with a password (see above).

OR

2 The system of the remote user or the system browser is verified according to X.509 so that the mGuard can use the X.509 authentication procedure. Further details must be specified here.

The use of option 1 or 2 depends on the web browser of the remote user.

Option 2 is used when the mGuard web browser provides a certificate.

### **Login with X.509 client certificate only**

The system of the remote user or the system browser must authenticate (verify) itself according to X.509 so that the mGuard can use the X.509 authentication procedure. Further details must be specified here.

☞ Before selecting the ***Login with X.509 client certificate only*** option, you must first select and test the ***Login with X.509 client certificate or password*** option. ***Login with X.509 client certificate only*** can only be used when this setting is fully functional. Otherwise you could be locked out of the system permanently!

This precautionary measure comes into force especially when settings are changed under **User authentication**.

If the following **User authentication methods** are defined:

- Login with X.509 client certificate only

OR

- Login with X.509 client certificate or password



then the process is defined with which the mGuard of the remote user is authenticated according to X.509.

The table below shows which certificates must be provided for the mGuard to authenticate the user (access over HTTPS) when the user or their browser displays one of the following certificate types on connection:

- A certificate signed by a CA
- A self-signed certificate

For further information on the following table see chapter “6.5.3 Authentication → Certificates” on page 150.

**X.509 authentication for HTTPS**

<b>The remote peer shows the following:</b>	Certificate (specific to individual) <b>signed by CA*</b>	Certificate (specific to individual) <b>self-signed</b>
<b>The mGuard authenticates the remote peer using:</b>		
	<p>All CA certificates that build the chain to the root CA certificate together with the certificates displayed by the remote peer</p> <p style="text-align: center;">or ADDITIONALLY</p> <p>Remote certificates, <u>if</u> used as filter</p>	Remote certificate

\* The remote peer can additionally provide sub-CA certificates. In this case the mGuard can form the set union for building the chain from the provided CA certificates and the self-configured CA certificates. The corresponding root certificate of the mGuard must always be available.

According to this table, the certificates must then be provided that the mGuard uses to authenticate a remote user (access over HTTPS) or their browser.

The following instructions assume that the certificates have been correctly installed in the mGuard. See “6.5.3 Authentication → Certificates” on page 150.

☒ If the use of block lists (CRL checking) is activated under the *Authentication → Certificate, Certificate settings* menu, then each certificate signed by a CA that shows a remote user is checked for blocks.

**CA certificate**

The configuration is only necessary when a user with HTTPS access displays a certificate signed by a CA.

All CA certificates needed by the mGuard to build the chain to the respective root CA certificate must be configured with the certificates displayed by the users.

If the browser of the remote user also provides CA certificates that contribute to building of the chain, then it is not necessary for the CA certificate to be installed and referenced at this point. However, the corresponding root CA certificate must be installed in the mGuard and made available (referenced) at all times.

☞ When selecting the CA certificates to be used, or when changing the selection or the filter settings, you must first select **Login with X.509 client certificate or password** as the *User authentication method* and test this before making the (new) setting effective. **Login restricted to X.509 client certificate** can only be used when this setting is fully functional. Otherwise you could be locked out of the system permanently!

This precautionary measure comes into force especially when settings are changed under **User authentication**.

**X.509 Subject**

Allows setting of a filter relating to the contents of the *Subject* field in the certificate displayed by the user. It is then possible to limit or grant access by users who would accept the mGuard in principle based on the certification check:

- Limitation to certain *subjects* (i.e. individuals) or to *subjects* that have certain attributes

OR

- Grant for all subjects

(See also glossary under “Subject, certificate”).)

The *X.509 subject* field must not be left empty.

**Grant for all subjects (individuals):**

With a \* in the *X.509 subject* field, you can define that all subject entries are allowed in the certificate displayed by the HTTPS client. Identification or definition of the subject in the certificate is then no longer needed.

**Limitation to certain subjects (individuals) or to subjects that have certain attributes:**

In the certificate, the certificate owner is entered in the *Subject* field. The entry is comprised of several attributes. These attributes are either expressed as an Object Identifier (e.g.: 132.3.7.32.1) or, more commonly, as an abbreviation with a relevant value.

Example: CN=John Smith, O=Smith and Co., C=UK

If certain subject attributes have very specific values for the acceptance of the user by the mGuard, then these must be specified accordingly. The values of the other freely selectable attributes are entered using the \* wildcard.

Example: CN=\*, O=\*, C=UK (with or without empty spaces between attributes)

In this example the attribute “C=UK” must be entered in the certificate under “subject”. Only then does the mGuard accept the certificate owner (subject) as a communication partner. The other attributes in the certificates to be filtered can have freely selectable values.

☞ If a subject filter is set, the number (but not the sequence) of the entered attributes must correspond to those of the certificates where the filter is to be used.

Pay attention to capitalization.

☞ Several filters can be set. Pay attention to the sequence! With HTTPS, the browser of the accessing user does not specify with which user or administration authorization it logs in. This access right allocation takes place here by setting filters (under “Authorized for access”). This has the following result: If there are several filters that “let through” a user, then the first filter comes into effect. The user receives the access rights as defined by this filter. This can vary from the access rights allocated to the user in the subsequent filter.

☞ If remote certificates are configured as filters in the **X.509 Certificate** table column, then these filters have priority over filter settings here.

**Authorized for access as: root / admin / netadmin / audit / user**

Defines which user or administrator rights are granted to the remote user.

For a description of the *root*, *admin* and *user* authorization levels, see “Authentication → Local Users” on page 146.

The *netadmin* and *audit* authorization levels relate to access rights with the Innominate Device Manager.

**X.509 Certificate**

Configuration is required in the following cases:

- Remote users each show a self-signed certificate.
- Remote users each show a certificate signed by a CA. Filtering should take place: Access is only granted to the user whose certificate copy is installed in the mGuard as the remote certificate and is provided in the mGuard table as *X.509 Certificate*.

If used, this filter has priority over the *Subject* filter in the table above.

The entry in this field defines which remote certificate the mGuard should adopt in order to authenticate the remote peer (browser of the remote user).

To do this, select one of the remote certificates from the selection list.

The selection list gives a selection of remote certificates that are loaded in the mGuard under the *Authentication → Certificate* menu.

**Authorized for access as: root / admin / netadmin / audit / user**

Defines which user or administrator rights are granted to the remote user.

For a description of the *root*, *admin* and *user* authorization levels, see “Authentication → Local Users” on page 146.

The *netadmin* and *audit* authorization levels relate to access rights with the Innominate Device Manager.

## 6.2.3 Management → Licensing

### Overview

Management » Licensing	
<div>Overview Install</div> <div>(mGuard Flash ID 000b000a40ffc77b-0142)</div>	
<b>AntiVirus License</b>	
AntiVirus license installed	yes
Expiry date	2007-06-01T16:15:32
<b>Feature License</b>	
<b>License with priority 1148898187</b>	
licence_id	0
licence_date	2006-05-29T10:23:07
flash_id	000b000a40ffc77b
serial_number	16529003
hardware_revision	00000dee
licence_order	264
product_code	51033
vpn_channels	-1
l2tp_server	1
snmp	1
remote_syslog	1
mau_management	1

☒ From mGuard version 5.0 onwards, licenses also remain installed after firmware is flashed.

Licenses are still deleted when devices with older firmware versions are flashed to version 5.0.0 or higher. Before flashing, the license for use of the new update must be obtained so the required license data is available for the flash.

This applies to major release upgrades, for example from version 4.x.x to version 5.x.x to version 6.x.x etc. See “Flashing the firmware” on page 249.

### AntiVirus License

#### AntiVirus license installed

Displays if an anti-virus license is installed.

#### Expiry date

Shows the expiry date of the installed anti-virus license.

### Feature License

Displays which functions are included with the installed mGuard license, e.g. the number of possible VPN tunnels, whether remote logging is supported etc.

## Install

The screenshot shows the 'Management > Licensing' window with the 'Install' tab selected. It contains two main sections: 'Automatic License Installation' and 'Manual License Installation'. The 'Automatic' section has a text input for 'Voucher Serial Number/Voucher Key' and two buttons: 'Online License Request' and 'Reload Licenses'. The 'Manual' section has a text input for 'Order License' with an 'Edit License Request Form' button, and a text input for 'Filename' with 'Browse...' and 'Install license file' buttons.

Afterwards, you can expand your installed mGuard license with further functions. A voucher serial number and key can be found in the voucher included with the mGuard. The voucher can also be purchased separately. With this you can perform the following functions:

1. Request the required feature license file
2. Install the license file

### Automatic License Installation

#### Voucher Serial Number / Voucher Key

Enter the serial number printed on the voucher and the corresponding voucher key, then click on **Online License Request**.

Result:

mGuard now establishes a connection via the Internet and installs the respective license on the mGuard if the voucher is valid.

#### Reload Licenses

Use this function if the license installed in the mGuard has been lost.

Click on the **Online License Reload** button.

The licenses that had been previously issued for the mGuard are then retrieved from the Internet and installed.

### Manual License Installation

#### Order License

After clicking the **Edit License Request Form** button, an online form is provided which can be used to order the desired license. In the request form, enter the following information:

**Voucher Serial Number:** The serial number printed on the voucher

**Voucher Key:** The voucher key on the voucher

**Flash ID:** Filled out automatically

After the form is submitted, the license file will be offered for download. You can then install the license file.

#### Filename (installing the license)

In order to apply a license, first save the license file as a separate file on your computer and continue as follows:

1. Click on the **Browse...** button next to the *Filename* field. Select the file and open it so that the file name or path is displayed in the *Filename* field.
2. Click on the **Install license file** button.

## 6.2.4 Management → Update

- ☒ From mGuard version 5.0.0 onwards, a license must be purchased for the affected device before the installation of a major release update (e.g. from version 4.x.y to 5.x.y or from version 5.x.y to 6.x.y). The license must be installed on the device before a firmware update is made (see “6.2.3 Management → Licensing”, “Install” on page 81).  
Minor release upgrades (i.e. same main version, e.g. within version 5.x.y) can be installed without a license until further notice.
- ☒ From firmware version 5.0 onwards, licenses also remain installed after firmware is flashed.

### Overview

Management » Update

Overview

Update

AntiVirus Pattern

System Information

Version

5.0.0.default

Base

5.0.0.default

Updates

[none]

AntiVirus Information

AntiVirus Engine Status

up

Last AntiVirus Update

main(50):25 Apr 2007 07:18 +0200  
daily(3475):20 Jun 2007 07:18 +0200  
63 seconds have passed since the last run of the update mechanism.  
The AntiVirus database is up to date.

AntiVirus Update Status

ok

Package Versions

Package	Number	Version	Flavour
bcrn	0	1.0.3	default
bootloader	0	1.3.3	default
bridge-utils	0	1.2.0	default
busybox	0	1.2.4	default
bzip2	0	0.1.0	default
chat	0	2.5.7	default
clamav	0	1.1.10	default

You can check the successful unblocking of the virus filter.

For information regarding the expiry date of your anti-virus license:

See “Management → Licensing” on page 80.

### System Information

#### Version

The current software version of the mGuard.

#### Base

The software version that was originally used to flash this mGuard.

#### Updates

List of updates that have been installed on the base.

### AntiVirus Information

#### AntiVirus Engine Status

Displays the state of the scan-engine. If monitoring is activated for at least one protocol, the status is displayed as **up**.

#### Last AntiVirus Update

Displays the version number and creation date of the virus signature.

#### AntiVirus Update Status

Displays if antivirus updates are activated, if the database update is being processed and if updates are blocked due to expiry of the antivirus license.

## Package Versions

Lists the individual software modules of the mGuard. Can be used for support purposes.

## Update

Protocol	Server	Login	Password
https://	update.innominat.com		

There are two possibilities for conducting a firmware update:

- You have the current package set file on your computer (the file name ends with “.tar.gz”) and you conduct a local update.

OR

- You download the package set file via the Internet from the update server and then install the packages.

- ☒ Depending on the size of the update, this may take several minutes.
- ☒ A message is displayed if a reboot is necessary after the update is completed.
- ☒ **Do not disconnect the power supply to the mGuard during the update procedure! The device could be damaged and may have to be reactivated by the manufacturer.**
- ☒ From mGuard version 5.0.0 onwards, a license must be purchased for the affected device before the installation of a major release update (e.g. from version 4.x.y to 5.x.y or from version 5.x.y to 6.x.y). The license must be installed on the device before a firmware update is made (see “6.2.3 Management → Licensing”, “Install” on page 81). Minor release upgrades (i.e. same main version, e.g. within version 5.x.y) can be installed without a license until further notice.

## Local Update

### Filename

To install the packages proceed as follows:

1. Click on the **Browse...** button. Select the file and open it so that the file name or path is displayed in the *Filename* field.  
The file name should have the following format: update-a.b.c-d.e.f.default.tar.gz.
2. Click on the **Install Packages** button.

## Online Update

To perform an online update, please proceed as follows:

1. Ensure that at least one valid entry exists under **Update Server**. You should have received the necessary details from your licensing authority.
2. Enter the package set name, e.g. “update-4.0.x-4.1.0”.
3. Click on the **Install Package Set** button.

### **Automatic Update**

This is a variation of the online update where the mGuard independently determines the required package set name.

#### **Install the latest patch release (x.y.Z)**

Patch releases resolve errors in previous versions and have a version number which only changes in the third digit position.

e.g. 4.0.1 is a patch release for version 4.0.0.

#### **Install the latest minor release (x.Y.z) for the currently installed major version**

#### **Install the next major release (X.y.z)**

Minor and major releases supplement the mGuard with new features or contain modifications in mGuard behavior. Their version number changes in the first and second digit position.

e.g. 4.1.0. is a major or minor release for versions 3.1.0 or 4.0.1.

### **Update Servers**

Here you can define from which servers the mGuard retrieves its updates.

- ☒ The list of servers is processed top-down until an available server is found. The sequence of the entries thus defines their priorities.

You have the following options:

#### **Protocol**

The update can be made using either HTTP or HTTPS.

#### **Server**

Hostname of the server that provides the update files.

#### **Login**

Login data for the server.

#### **Password**

Password for the login.

**AntiVirus Pattern**

(Only displayed when a virus filter is installed and licensed)

Management » Update

Overview Update **AntiVirus Pattern**

**Schedule**

Update Schedule Never

**Update Servers for AVP**

Update Location (Hostname)
downloads.avp.innomir

**Proxy Settings**

HTTP Proxy Server	Port	Login	Password

The virus signature files (also known as *anti-virus pattern* or *virus identification pattern*) can be updated from a selected update server at intervals defined by the user. The update is performed without interrupting the operation of the anti-virus filter. The mGuard is delivered without any virus signatures installed. Therefore, after the anti-virus protection has been activated with the corresponding license, you should also set the update schedule. The course of the updates can be examined in the anti-virus update log.

**Schedule****Update Schedule**

Enter here if and in which intervals an automatic update of the virus identification pattern should take place. To do this, open the selection list and select the desired value.

The database has a size of several MB. Only files updated on the server are loaded.

**Update Servers for AVP**

Enter at least one AVP update server name here.

You can select the server from which the updated signature files should be downloaded. A default server is already entered. If needed, you can enter your own servers.

- ☒ The list of servers is processed top-down until an available server is found. The sequence of the entries thus defines their priorities.

**Proxy Settings****HTTP Proxy Server**

When using a HTTP proxy server, enter here the IP address and the **Port** number used. Enter the user name and password under **Login** and **Password**.

## 6.2.5 Management → Configuration Profiles

### Configuration Profiles

You can save the configuration settings of the mGuard as a configuration profile under any name in the mGuard. It is possible to create and save multiple configuration profiles. You may then switch between different profiles, for example, if the mGuard is used in different operating environments.

Furthermore, you can also save configuration profiles as files on the configuration system. Alternately, these configuration files can then be read back onto the mGuard and activated.

You can restore the mGuard to the *factory default* at any time.

Configuration profiles on the EAGLE mGuard can also be stored on an automatic configuration adaptor (ACA) that can be connected to the V.24/USB port of the mGuard – see “Profiles on the ACA (EAGLE mGuard only)” on page 87.

☒ When a configuration profile is saved, the passwords used for the authentication of administrative access to the mGuard are not saved.

### Configuration Profiles

The top of the *Configuration Profiles* page has a list of configuration profiles that are stored on the mGuard, for example, the *Factory Default* configuration profile. If any configuration profiles have been saved by the user (see below), they will be listed here.

**Active configuration profile:** The configuration profile currently in effect has an *Active* symbol at the front of the entry.

You can perform the following with configuration profiles that are stored on the mGuard:

- Activate them
- Save them to a file on the connected configuration computer
- Delete them
- Display them

### Displaying the configuration profile

Click the name of the configuration profile in the list.

**Applying the factory defaults or a configuration profile stored by the user**

Click the **Restore** button located to the right of the name of the relevant configuration profile.

Result:

The corresponding configuration profile is activated.

- ☒ If the restore process involves a switch between Stealth mode and another network mode, then mGuard is restarted.

**Saving the configuration profile as a file to the configuration computer**

1. Click the **Download** button located to the right of the relevant configuration profile.
2. Specify the file name and folder in which the configuration profile is to be saved as a file in the displayed text field.

The file name is freely selectable.

**Deleting a configuration profile**

Click the **Delete** button located to the right of the relevant configuration profile.

- ☒ The **Factory Default** profile cannot be deleted.

**Saving the current configuration as a configuration profile on the mGuard**

1. Enter the desired profile name in the *Name for new profile* field behind “Save Current Configuration to Profile”.
2. Click on the **Save** button.

Result:

The configuration profile is saved in the mGuard, and the profile name is displayed in the list of profiles saved in the mGuard.

**Uploading a configuration profile that has been saved to the configuration computer file**

**Requirement:** You have saved a configuration profile on the configuration computer as a file according to the procedure described above.

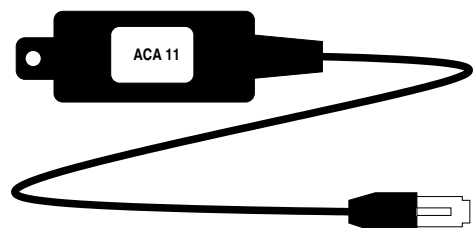
1. Enter the desired profile name in the *Name for new profile* field behind “Upload Configuration to Profile”.
2. Click on the **Browse...** button. Select the file and open it so that the file name or path is displayed in the dialog.
3. Click on the **Upload** button.

Result:

The configuration profile is loaded on the mGuard. The name assigned in step 1 is displayed in the list of the profiles stored on the mGuard.

**Profiles on the ACA (EAGLE mGuard only)**

Configuration profiles can also be stored on an external auto-configuration adaptor (ACA). Connect the ACA to the V.24 (ACA11) or USB (ACA21) port of the EAGLE mGuard.



### Storing a profile on the ACA

1. When the password of the EAGLE mGuard where the profile is imported has a different root password than “root”, then you must enter this under **The root password to save on ACA.**
2. Click on the **Save** button.

Result:

The LED STATUS (and the V.24 LED for ACA11) flashes until the store procedure is finished.

### Restoring a profile from the ACA

Plug the ACA into the EAGLE mGuard V.24 port. Start the EAGLE mGuard whilst the ACA is plugged in. The mGuard password must be either “root” or correspond to the password designated when storing the profile.

The LED STATUS (and the V.24 LED for ACA11) flashes until the load procedure is finished.

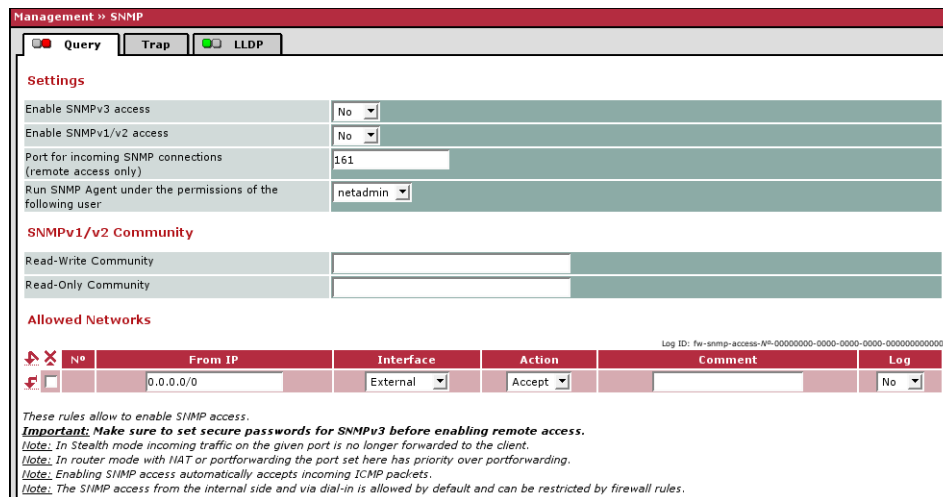
Result:

The configuration profile loaded from the ACA is loaded into the EAGLE mGuard and started. It does not appear in the list of configuration profiles stored on the EAGLE mGuard.

- ☒ The configuration on the ACA also includes the *root*, *admin* and *user* passwords. These are also used when restoring a configuration from the ACA.

## 6.2.6 Management → SNMP

### Query



Management → SNMP

☒ Query ☐ Trap ☐ LLDP

**Settings**

Enable SNMPv3 access

Enable SNMPv1/v2 access

Port for incoming SNMP connections (remote access only)

Run SNMP Agent under the permissions of the following user

**SNMPv1/v2 Community**

Read-Write Community

Read-Only Community

**Allowed Networks**

N#	From IP	Interface	Action	Comment	Log
1	0.0.0.0/0	External	Accept		No

Log ID: fw-snmp-access-N#-00000000-0000-0000-0000-000000000000

These rules allow to enable SNMP access.

**Important:** Make sure to set secure passwords for SNMPv3 before enabling remote access.

Note: In Stealth mode incoming traffic on the given port is no longer forwarded to the client.

Note: In router mode with NAT or portforwarding the port set here has priority over portforwarding.

Note: Enabling SNMP access automatically accepts incoming ICMP packets.

Note: The SNMP access from the internal side and via dial-in is allowed by default and can be restricted by firewall rules.

SNMP (Simple Network Management Protocol) is mainly used in more complex networks to monitor the status and operation of devices.

SNMP is available in several firmware versions: SNMPv1/SNMPv2 and SNMPv3.

The older versions (SNMPv1/SNMPv2) do not use encryption and are not considered to be secure. We therefore do not recommend using SNMPv1/SNMPv2.

SNMPv3 is considerably better from a security perspective, but not all management consoles support it.

If SNMPv3 or SNMPv1/v2 is enabled, this is indicated by a green signal field on the tab at the top of the page. Otherwise – i.e. if SNMPv3 and SNMPv1/v2 are not enabled – the signal field is red.

☒ It can take more than one second to process SNMP “get” or “walk” requests.

However, the standard timeout value of many SNMP management applications is set to one second.

In case you experience timeout problems, please set the time-out of your management application to values between 3 and 5 seconds.

### Settings

#### Enable SNMPv3 access: Yes / No

If you wish to allow monitoring of the mGuard via SNMPv3, set this option to **Yes**.

☞ You must define the firewall rules for the available interfaces on this page under **Allowed networks** in order to specify access and monitoring possibilities for the mGuard.

Access via SNMPv3 requires authentication with a login and password. The factory defaults for the login parameters are:

**Login:** admin

**Password:** SnmpAdmin (please pay attention to capitalization!)

MD5 is supported for the authentication process; DES is supported for encryption.

The login parameters for SNMPv3 can only be changed using SNMPv3.

**Enable SNMPv1/v2 access: Yes / No**

If you wish to allow monitoring of the mGuard via SNMPv1/v2, set this option to **Yes**.

You must also enter your login data under **SNMPv1/v2 Community**.

☞ You must define the firewall rules for the available interfaces on this page under **Allowed networks** in order to specify access and monitoring possibilities for the mGuard.

**Port for SNMP connections**

Standard: 161

If this port number is changed, the new port number only applies for access over the *External*, *External 2* and *VPN* interfaces and over *Dial-in*.

Port number 161 still applies for internal access.

The remote peer making the remote access may have to enter the port number defined here when entering the address.

**SNMPv1/v2 Community****Read-Write Community****Read-Only Community**

Enter the required login data in these fields.

**Allowed Networks**

Lists the firewall rules that have been set. These apply for incoming data packets of an SNMP access.

The rules specified here only become effective if **Enable SNMPv3 access** or **Enable SNMPv1/v2 access** is set to **Yes**.

If multiple firewall rules are set, they will be searched in the order in which they are listed (top-down) until a suitable rule is found. This rule is then applied. If there are other suitable rules further down the list, then these are ignored.

**From IP**

In this field you enter the address of the system or network where remote access is permitted or forbidden.

You have the following options:

- An IP address
- To enter an address, use CIDR notation – see “CIDR (Classless Inter-Domain Routing)” on page 246.
- **0.0.0.0/0** means all addresses.

**Interface**

**External / Internal / External 2 / VPN / Dial-in<sup>1</sup>**

Specifies which interface the rules apply to.

If no rules are set, the following default settings apply:

SNMP monitoring is permitted over *Internal*, *VPN* and *Dial-in*.

Access over *External* and *External 2* is refused.

If required, you can specify the monitoring possibilities.

---

1. *External 2* and *Dial-in* only for devices with serial ports.  
See “Network → Interfaces” on page 105.

**Caution:**

If you want to refuse access over *Internal*, *VPN* or *Dial-in*, you must implement this explicitly through corresponding firewall rules, by specifying *Drop* as an action, for example. To avoid locking yourself out, you may have to simultaneously allow access over another interface explicitly with *Accept* before you make the new setting effective by clicking the **Apply** button. Otherwise, if you are locked out, you must perform the recovery procedure.

**Action**

Possible settings:

- Accept
- Reject
- Drop

**Accept** means that data packets may pass through.

**Reject** means that the data packets are rejected. The sender is informed that the data packets have been rejected. In *Stealth* mode, *Reject* has the same effect as *Drop*.

**Drop** means that data packets may not pass through. The data packets are discarded and the sender is not informed of their whereabouts.

**Comment**

Freely selectable comment for this rule.

**Log**

For each individual firewall rule you can specify whether the use of the rule

- should be logged (set *Log* to **Yes**) or
- should not be logged (set *Log* to **No** – factory default).

## Trap

The screenshot shows the 'Management - SNMP' configuration page. It has tabs for 'Query', 'Trap', and 'LLDP'. The 'Trap' tab is active. The page is divided into sections for different trap types, each with a 'Yes' or 'No' dropdown menu. The sections are: Basic traps (SNMP authentication, Link Up/Down, Coldstart, Admin access), Hardware related traps (Chassis, Agent), Anti-virus traps (Successful update, AV update, Found virus), Redundancy traps (Status change), Userfirewall traps (Userfirewall traps), VPN traps (IPsec connection, L2TP connection), and SEC-Stick Traps (SEC-Stick connection). At the bottom, the 'Trap destinations' table is shown with one entry: Destination IP: 0.0.0.0, Destination Port: 162, Destination Name: (empty), Destination Community: (empty). A small note at the bottom states: 'Platform-specific configurations are only effective on the platform in question. Similarly AV traps are only sent when a licensed anti-virus system is active. SNMP-traps only are sent if SNMP access is enabled.'

In certain cases the mGuard can send SNMP traps (→ Glossary).

Traps correspond to SNMPv1. The following list details the trap information for each setting. The exact description can be found in the MIB belonging to the mGuard.

### Basic traps

- SNMP authentication:** Activate traps **Yes / No**  
 enterprise-oid : mGuardInfo  
 generic-trap : authenticationFailure  
 specific-trap : 0  
*Explanation* : Sent if an unauthorized station tries to access the mGuard SNMP agents.
- Link Up/Down:** Activate traps **Yes / No**  
 enterprise-oid : mGuardInfo  
 generic-trap : linkUp, linkDown  
 specific-trap : 0  
*Explanation* : Sent when the connection to a port is interrupted (linkDown) or restored (linkUp).
- Coldstart:** Activate traps **Yes / No**  
 enterprise-oid : mGuardInfo  
 generic-trap : coldStart  
 specific-trap : 0  
*Explanation* : Sent after cold or warm start.
- Admin access (SSH, HTTPS), new DHCP client:** Activate traps **Yes / No**  
 enterprise-oid : mGuardb  
 generic-trap : enterpriseSpecific  
 specific-trap : mGuardHTTPSLoginTrap (1)  
 additional : mGuardHTTPSLastAccessIP  
*Explanation* : Sent when someone tries to open a HTTPS session using an incorrect password.  
 The trap contains the IP address of the last unsuccessful login request attempt.

enterprise-oid : mGuard  
 generic-trap : enterpriseSpecific  
 specific-trap : mGuardShellLoginTrap (2)  
 additional : mGuardShellLastAccessIP  
*Explanation* : Sent when someone opens the shell  
 using SSH or the serial port. The trap contains  
 the IP address of the login request. If this request  
 is made over the serial port then the value is 0.0.0.0.

enterprise-oid : mGuard  
 generic-trap : enterpriseSpecific  
 specific-trap : 3  
 additional : mGuardHTTPSLastAccessMAC  
*Explanation* : Sent when a DHCP request from  
 an unknown client is received.

#### Hardware-related traps (mGuard industrial RS and EAGLE mGuard only)

- **Chassis (power supply, relay):** Activate traps **Yes / No**

enterprise-oid : mGuardTrapSenderIndustrial  
 genericTrap : enterpriseSpecific  
 specific-trap : mGuardTrapIndustrialPowerStatus (2)  
 additional : mGuardTrapIndustrialPowerStatus  
*Explanation* : Sent when the system registers  
 a power outage.

enterprise-oid : mGuardTrapSenderIndustrial  
 genericTrap : enterpriseSpecific  
 specific-trap : mGuardTrapSignalRelais (3)  
 additional : mGuardTResSignalRelaisState  
 (mGuardTEsSignalRelaisReason, mGuardTResSignal  
 RelaisReasonIdx)  
*Explanation* : Sent after the signal contact is changed and displays  
 the current status (0 = Off, 1 = On).

- **Agent (ACA, temperature):** Activate traps **Yes / No**

enterprise-oid : mGuardTrapIndustrial  
 genericTrap : enterpriseSpecific  
 specific-trap : mGuardTrapIndustrialTemperature (1)  
 additional : mGuardSystemTemperature,  
 mGuardTrapIndustrialTempHiLimit,  
 mGuardTrapIndustrialLowLimit  
*Explanation* : Displays the temperature when defined  
 limits are exceeded.

enterprise-oid : mGuardTrapIndustrial  
 genericTrap : enterpriseSpecific  
 specific-trap : mGuardTrapAutoConfigAdapterState (4)  
 additional : mGuardTrapAutoConfigAdapterChange  
*Explanation* : Sent following access to the ACA.

**Blade controller traps (blade only)**

- **Blade status change** (blade switch, outage): Activate traps **Yes / No**

enterprise-oid : mGuardTrapBladeCTRL  
generic-trap : enterpriseSpecific  
specific-trap : mGuardTrapBladeCtrlPowerStatus (2)  
additional : mGuardTrapBladeRackID,  
mGuardTrapBladeSlotNr,  
mGuardTrapBladeCtrlPowerStatus

*Explanation* : Sent when the power supply status of the blade pack changes.

enterprise-oid : mGuardTrapBladeCTRL  
generic-trap : enterpriseSpecific  
specific-trap : mGuardTrapBladeCtrlRunStatus (3)  
additional : mGuardTrapBladeRackID,  
mGuardTrapBladeSlotNr,  
mGuardTrapBladeCtrlRunStatus

*Explanation* : Sent when the blade run status changes.

- **Blade reconfiguration** (backup / restore): Activate traps **Yes / No**

enterprise-oid : mGuardTrapBladeCtrlCfg  
generic-trap : enterpriseSpecific  
specific-trap : mGuardTrapBladeCtrlCfgBackup (1)  
additional : mGuardTrapBladeRackID,  
mGuardTrapBladeSlotNr,  
mGuardTrapBladeCtrlCfgBackup

*Explanation* : Sent when blade controller configuration backup is completed.

enterprise-oid : mGuardTrapBladeCtrlCfg  
generic-trap : enterpriseSpecific  
specific-trap : mGuardTrapBladeCtrlCfgRestored 2  
additional : mGuardTrapBladeRackID,  
mGuardTrapBladeSlotNr,  
mGuardTrapBladeCtrlCfgRestored

*Explanation* : Sent when blade controller configuration restoration is completed.

**Anti-Virus traps**

- **Successful update of AV pattern:** Activate traps **Yes / No**

enterprise-oid : mGuardTrapAv  
generic-trap : enterpriseSpecific  
specific-trap : mGuardTrapAvUpdateDone (1)  
additional : mGuardTResAvUpdateDone

*Explanation* : Sent after successful AV update.

- **AV update or scanning problem:** Activate traps **Yes / No**

enterprise-oid : mGuardTrapAv  
generic-trap : enterpriseSpecific  
specific-trap : mGuardTrapAvUpdateError (2)  
additional : mGuardTResAvUpdateError

*Explanation* : Sent when an error occurs during the AV update.

enterprise-oid : mGuardTrapAv  
 generic-trap : enterpriseSpecific  
 specific-trap : mGuardTrapAvFailed (5)  
 additional : mGuardTResAvFailed  
*Explanation* : Sent during a general AV error.

- **Found virus or skipped scanning:** Activate traps **Yes / No**

enterprise-oid : mGuardTrapAv  
 generic-trap : enterpriseSpecific  
 specific-trap : mGuardTrapAvVirusDetected (3)  
 additional : mGuardTResAvVirusDetected  
*Explanation* : Sent when virus is found by the AV function.

enterprise-oid : mGuardTrapAv  
 generic-trap : enterpriseSpecific  
 specific-trap : mGuardTrapAvFileNotScanned (4)  
 additional : mGuardTResAvFileNotScanned  
*Explanation* : Sent when file has not been scanned for viruses.

### Redundancy traps

- **Status change:** Activate traps **Yes / No**

enterprise-oid : mGuardTrapRouterRedundancy  
 genericTrap : enterpriseSpecific  
 specific-trap : mGuardTrapRouterRedStatusChange TRAP-TYPE (1)  
 additional : mGuardTResRedundancyState,  
                   mGuardTResRedundancyReason  
*Explanation* : Sent after change in current HA cluster status.

enterprise-oid : mGuardTrapRouterRedundancy  
 genericTrap : enterpriseSpecific  
 specific-trap : mGuardTrapRouterRedBackupDown TRAP-TYPE (2)  
 additional : mGuardTResRedundancyBackupDown  
*Explanation* : Sent when the master device cannot reach  
                   the backup device (only sent when  
                   ICMP checks are activated).

### Userfirewall traps: Yes / No

enterprise-oid : mGuardTrapUserFirewall  
 generic-trap : enterpriseSpecific  
 specific-trap : mGuardTrapUserFirewallLogin (1)  
 additional : mGuardTResUserFirewallUsername,  
                   mGuardTResUserFirewallSrcIP,  
                   mGuardTResUserFirewallAuthenticationMethod  
*Explanation* : Sent when user logs in to a user firewall.

enterprise-oid : mGuardTrapUserFirewall  
 generic-trap : enterpriseSpecific  
 specific-trap : mGuardTrapUserFirewallLogout (2)  
 additional : mGuardTResUserFirewallUsername,  
                   mGuardTResUserFirewallSrcIP,  
                   mGuardTResUserFirewallLogoutReason  
*Explanation* : Sent when user logs out of a user firewall.

enterprise-oid : mGuardTrapUserFirewall  
generic-trap : enterpriseSpecific  
specific-trap : mGuardTrapUserFirewallAuthError TRAP-TYPE (3)  
additional : mGuardTResUserFirewallUsername,  
mGuardTResUserFirewallSrcIP,  
mGuardTResUserFirewallAuthenticationMethod  
*Explanation* : Sent during an authentication error.

### VPN traps

- **Status change of IPsec connections: Yes / No.**

enterprise-oid : mGuardTrapVPN  
genericTrap : enterpriseSpecific  
specific-trap : mGuardTrapVPNIKEServerStatus (1)  
additional : mGuardTResVPNStatus  
*Explanation* : Sent during starting and stopping of IPsec IKE servers

enterprise-oid : mGuardTrapVPN  
genericTrap : enterpriseSpecific  
specific-trap : mGuardTrapVPNIPsecConnStatus (2)  
additional : mGuardTResVPNName, mGuardTResVPNIndex,  
mGuardTResVPNPeer, mGuardTResVPNStatus,  
mGuardTResVPNTType, mGuardTResVPNLocal,  
mGuardTResVPNRemote  
*Explanation* : Sent when the state of an IPsec connection changes

- **Status change of L2TP connections: Yes / No.**

enterprise-oid : mGuardTrapVPN  
genericTrap : enterpriseSpecific  
specific-trap : mGuardTrapVPNL2TPConnStatus (3)  
additional : mGuardTResVPNName, mGuardTResVPNIndex,  
mGuardTResVPNPeer, mGuardTResVPNStatus,  
mGuardTResVPNLocal, mGuardTResVPNRemote  
*Explanation* : Sent when the state of an L2TP connection changes

### SNMP trap destinations

Traps can be sent to one or more targets.

#### Destination IP

IP address to which the trap should be sent.

#### Destination Port

Standard: 162

Destination port to which the trap should be sent.

#### Destination Name

Optional name for the destination. Has no influence on the generated traps.

#### Destination Community

Name of the SNMP community allocated to the trap.

LLDP

Management » SNMP

Query

Trap

LLDP

LLDP

Mode

Enabled

Internal/LAN interface

Chassis ID	IP address	Port description	System name
------------	------------	------------------	-------------

External/WAN interface

Chassis ID	IP address	Port description	System name
MAC: 00 0C BE 02 21 2C	(none)	WAN port	rambaldi
MAC: 00 0C BE 01 32 E1	10.1.0.254	LAN port	devel-mguard
MAC: 00 0C BE 02 36 F1	(none)	WAN port	mguard
MAC: 00 0C BE 01 0E D5	10.1.200.1	WAN port	qa-mguard

Update

LLDP (Link Layer Discovery Protocol, IEEE 802.1AB/D13) supports the automatic detection of (ethernet) network topology using suitable request methods. LLDP capable devices periodically send ethernet multicasts (layer 2). Tables of systems connected to the network are created from their answers, which can then be requested using SNMP.

LLDP

Mode: Enabled / Disabled

The LLDP service or agent can be enabled or disabled here. If the function is enabled, this is indicated by a green signal field on the tab at the top of the page. If the signal field is red, the function is disabled.

Internal / LAN interface

and

External / WAN interface

Chassis ID

A unique ID of the found system; typically one of its MAC addresses.

IP address

The IP address of the found system with which SNMP administration can be made.

Port description

A textual description of the network interface where the system was found.

System name

Hostname of the found system.

Buttons

Update

Click on **Update** to update the displayed data.

## 6.2.7 Management → Central Management

### Configuration Pull

Configuration Pull	
Pull Schedule	Never
Server	config.example.com
Directory	
Filename (When empty, '2T900054.atv' will be used.)	
Number of times a configuration profile is ignored after it was rolled back	2
Download timeout (seconds)	120
Login	anonymous
Password	*****
Server Certificate (The server's certificate is needed here if and only if it is self signed. Otherwise, the root certificate of the CA which issued the server's certificate must be installed.)	No certificate installed  Browse... Import
Download Test	No certificate installed  Test Download

The mGuard can retrieve new configuration profiles from a HTTPS server in configurable time intervals, provided that the server makes them available as files for the mGuard (file ending: .atv). When a new mGuard configuration differs from the current configuration, it will be downloaded and activated automatically.

### Configuration Pull

#### Pull Schedule

Enter here if (and if so, when and in which intervals) the mGuard should attempt to download and apply a new configuration from the server. To do this, open the selection list and select the desired value.

A new text field opens when **Time Schedule** is selected. Enter here whether the new configuration should be downloaded daily or repeatedly on a certain weekday and at which time.

The time-controlled download of a new configuration can only be made after synchronization of the system time – see “Management → System Settings”, “Time and Date” on page 62.

Time control sets the selected time related to the configured time zone.

#### Server

IP or hostname of the server that provides the configuration profiles.

#### Directory

The directory (folder) on the server where the configuration is located.

#### Filename

The name of the file in the directory defined above. If no filename is defined here, the serial number of the mGuard is used, including the ending “.atv”.

**Number of times a configuration profile is ignored after it was rolled back**

Standard: 10

After a new configuration is retrieved it can occur that the mGuard is no longer accessible after the configuration is put into force. A new remote configuration for correction purposes is then no longer possible. In order to rule this out, the mGuard makes the following checks:

After the retrieved configuration is enforced, the mGuard tries to connect again to the configuration server based on the new configuration. The mGuard then attempts to download the newly enforced configuration once again.

If this is successful, the new configuration remains.

If unsuccessful for whatever reason, the mGuard assumes that the newly enforced configuration profile is defective. The mGuard memorizes the MD5 total for identification purposes, and then performs a rollback. Rollback means that the last (working) configuration is restored. This assumes that the new (non-functioning) configuration contains a rollback instruction when the new configuration profile is defective according to the check procedure detailed above.

When the mGuard attempts to retrieve a new configuration profile cyclically after the time defined in **Pull Schedule** (and **Time Schedule**), it will only accept the profile under the following selection criteria: The provided configuration profile must vary from the configuration profile identified as defective that led to the rollback. To do this, the mGuard checks the old MD5 total (i.e. of the defective configuration) against the MD5 total of the suggested new configuration profile.

If these selection criteria are fulfilled (i.e. the new configuration profile is offered), then the mGuard retrieves this configuration profile, enforces it and checks it according to the procedure detailed above. It also disables it if the rollback check is negative.

If the selection criteria are not fulfilled (i.e. same configuration profile is offered), then the cyclical request of these criteria remains in force for the period defined in **Number of times...** If the defined number of times expires without a change of the configuration profile on the server, then the mGuard enforces the unchanged new (defective) configuration profile once more, despite it being defective. This occurs to rule out external factors (e.g. network outage) for the check failure. The mGuard then once again attempts to connect to the configuration server based on the new configuration, and then downloads the newly enforced configuration profile. If this is unsuccessful, then another rollback is made. The selection criteria is enforced for further load cycles for the period defined in **Number of times...**

If the value **0** is defined in the **Number of times...** field, then the selection criteria will never come into effect (the offered configuration profile is ignored if it remains unchanged). As a result, the second of the following goals can then no longer be reached.

This mechanism has the following goals:

1. After enforcing the new configuration, the mGuard must still be configurable from a remote location.
2. When cycles are close together (e.g. **Schedule** = 15 minutes), the mGuard must be prevented from testing a possibly defective configuration profile over and over in such a short space of time. This can lead to blocking of external administrative access, as the mGuard is busy dealing with its own processes.
3. External factors (e.g. network outage) must be ruled out as a reason for the mGuard's consideration of a defective configuration.

☞ An application note is provided by Innominate. This contains a description of how a rollback can be started using a configuration profile.

### **Download timeout (seconds)**

Standard: 120. Defines after how long a timeout is made during the download of a configuration file (i.e. when no action is taken). The download is canceled if this time is exceeded. If and when a new download attempt is made can be seen in the *Schedule* setting (see above).

### **Login**

The login (user name) on the HTTPS server.

### **Password**

The password on the HTTPS server.

### **Server Certificate**

The certificate that the mGuard uses to check the authentication of the certificate suggested by the configuration server. It is used to prevent unauthorized configurations from being installed on the mGuard.

The following may be entered here:

- A self-signed certificate of the configuration server (i.e. the remote certificate of the self-signed configuration server machine certificate)

OR

- The root certificate of the CA that created the server certificate. This is valid when the configuration server certificate is signed by a CA (instead of a self-signed one).

☞ If the configuration profiles also contain the private VPN key for VPN connections or VPN connections with PSK, then the following conditions must be fulfilled:

- The password should consist of at least 30 random upper and lower case letters and numbers (prevention of unauthorized access).
- The HTTPS server should only grant access to this individual mGuard using the login and password. Otherwise, users can access other mGuards.

☞ The IP address or the hostname specified under *Server* must be the same as the certificate's Common Name (CN).

☞ Self-signed certificates should not use the “key-usage” extension.

To install a certificate, please proceed as follows:

Requirement:

The certificate file is saved on the connected computer

1. Click on **Browse...** to select the file.
2. Click on **Import**.

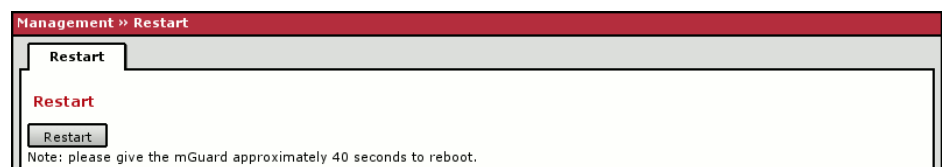
### Download Test

By clicking on **Test Download** you can test if the parameters are correct without actually saving the modified parameters or activating the profile. The result of the test is displayed in the right column.

- ☒ Ensure that the profile on the server does not contain unwanted variables beginning with “GAI\_PULL\_”, as these overwrite the set configuration.

## 6.2.8 Management → Restart

### Restart



Restarts the mGuard. Has the same effect as a power outage. The mGuard is turned off and on again.

A restart (reboot) is necessary in case of errors. This may also be necessary after a software update.

## 6.3 Blade Control Menu (control unit only)

This menu is only available on the blade control unit.

### 6.3.1 Blade Control → Overview

Blade Control » Overview									
Overview									
Rack ID	0								
Power supply P1	Defect								
Power supply P2	OK								
Blade	Device	Status	WAN	LAN	Serial	Version	B	R	
01	blade	Online	Down	Up	2TN00053	4.2.0.default			
02	blade XL	Online	Up	Down	2T500146	5.0.0-pre02+.def			
03	blade	Online	Down	Down	2T500083	2.3.0.default			
04	Unknown	Present							
05	blade	Online	Down	Down	2TN00051	4.2.0.default			
06	blade XL	Online	Down	Down	2T600005	4.2.0-pre08-beta			
07	blade	Online	Down	Down	2T500161	4.2.0-pre05-beta			
08	blade	Online	Down	Down	2TN00050	4.2.0-pre05-beta			
09	Unknown	Absent							
10	Unknown	Absent							
11	Unknown	Absent							
12	Unknown	Absent							

[B] Automatic configuration backup is enabled/disabled  
[R] Automatic reconfiguration of a replaced blade is enabled/disabled

#### Rack ID

The ID of the rack where the mGuard is mounted. This value can be configured for all blades on the control unit.

#### Power supply P1/P2

State of the power supplies P1 and P2.

- OK
- Absent
- Defect
- Fatal error

#### Blade

Number of the slot where the mGuard is installed.

#### Device

Device name, e.g. “blade” or “blade XL”.

#### Status

**Online** – The device in the slot is working correctly.

**Present** – Device is present but not yet ready (e.g. in start-up phase).

**Absent** – No device found in the slot.

#### WAN

Status of the WAN port.

#### LAN

Status of the LAN port.

#### Serial number

The serial number of the mGuard.

#### Version

The software version of the mGuard.

**B**

**Backup:** Automatic configuration backup on the controller is activated/deactivated for this slot.

**R**

**Restore:** Automatic configuration restoration after replacing the mGuard is activated/deactivated for this slot.

### 6.3.2 Blade Control → Blade 01 to 12

These pages show the status information of each installed mGuard and allow the configuration backup and restoration of the respective mGuard.

#### Blade in slot #...

Blade Control » Blade 01	
Blade in slot #01	Configuration
<b>Overview</b>	
Device type	blade
ID bus controller ID	[0x24] [0x1] [0x1] [0x2]
Serial number	2TN00053
Flash ID	0031000141ad42a2
Software version	4.2.0.default
MAC addresses	[00:0c:be:02:2c:88] [00:0c:be:02:2c:89] [00:0c:be:02:2c:8a] [00:0c:be:02:2c:8b]
Status	Online
LAN link status	Up
WAN link status	Down
Temperature	43.50°C

#### Device type

Device name, e.g. “blade” or “blade XL”.

#### ID bus controller ID

ID of this slot on the bladeBases control bus.

#### Serial number

The serial number of the mGuard.

#### Flash ID

Flash ID of the mGuard’s flash chip.

#### Software version

Software version installed on the mGuard.

#### MAC addresses

All MAC addresses used by the mGuard.

#### Status

Status of the mGuard.

#### LAN link status

Status of the LAN port.

#### WAN link status

Status of the WAN port.

## Configuration

The screenshot shows a web interface titled "Blade Control » Blade 01". It has two tabs: "Blade in slot #01" and "Configuration". The "Configuration" tab is active, showing a status message "Configuration [ No configuration file ]". Below this, there are several sections:

- Configuration backup [Blade #01 -> Controller]**: Includes a "Manual" dropdown menu, a "Backup" button, and a "Restore" button.
- Reconfiguration, if Blade #01 is replaced**: Includes a "Manual" dropdown menu.
- Delete configuration backup of Blade #01**: Includes a "Delete" button.
- Upload configuration from client**: Includes a text input field, a "Browse..." button, and an "Upload from client" button.
- Download configuration to client**: Includes a "Download to client" button.

### Configuration backup [Blade #\_\_ -> Controller]

**Automatic:** The new configuration is stored automatically on the controller shortly after a configuration change on the mGuard.

**Manual:** The configuration can be stored on the controller using the **Backup** button and can be restored on the mGuard using the **Restore** button.

### Reconfiguration, if Blade #\_\_ is replaced

After replacing an mGuard in this slot, the configuration stored on the controller will be automatically transferred to the new mGuard.

### Delete configuration backup of Blade #\_\_

Deletes the configuration stored on the controller for this slot.

### Upload configuration from client

Uploads and saves a configuration profile for this slot onto the controller.

### Download configuration to client

Downloads the configuration profile stored on the controller for this slot onto the configuration PC.

## 6.4 Network Menu

### 6.4.1 Network → Interfaces

The mGuard has the following interfaces with external access:

	Ethernet: Internal: LAN External: WAN	Serial ports	Built-in Modem
mGuard Smart	<b>Yes</b>	<b>No</b>	<b>No</b>
mGuard industrial RS, mGuard blade, EAGLE mGuard, mGuard delta	<b>Yes</b>	<b>Yes</b>	<b>No</b>
Optional: mGuard industrial RS	<b>Yes</b>	<b>Yes</b>	<b>Yes</b>

The LAN port is connected to a single computer or to the local network (= internal). The WAN port is for the connection to the external network. For devices with a serial interface, the connection to the external network can also or additionally be made over the serial interface. Alternatively, the serial port can be used as follows: for PPP dialin to the local network or for configuration purposes. For devices with a built-in modem (analog modem or ISDN terminal adaptor), the modem can be used additionally to combine access possibilities.

The details for this must be configured on the *General*, *Ethernet*, *Outgoing Call*, *Incoming Call* and *Modem / Console* tab pages. For further explanations of the possibilities for using the serial ports (and a built-in modem) see “Modem / Console” on page 133.

**Network → Interfaces**

General | **Ethernet** | Dial-out | Dial-in | Modem / Console

**Network Status**

External IP address: Primary: 192.168.66.1  
Secondary: (not in use)

Active Defaultroute: (none)

Used DNS servers: DNS Root Servers

**Network Mode**

Network Mode: Router

**External Networks**

Obtain external configuration via DHCP: No

External IPs (untrusted port)

IP	Netmask	Use VLAN	VLAN ID
10.0.0.152	255.255.255.0	No	1

Additional External Routes

Network	Gateway
10.0.0.253	

IP of default gateway: 10.0.0.253

**Internal Networks**

Internal IPs (trusted port)

IP	Netmask	Use VLAN	VLAN ID
192.168.1.1	255.255.255.0	No	1

Additional Internal Routes

Network	Gateway
---------	---------

**Secondary External Interface**

Network Mode: Modem

Operation Mode: temporary

Secondary External Routes

Network	Gateway
---------	---------

## General

### Network Status

#### External IP address (WAN port address)

Display only: The addresses through which the mGuard can be accessed by devices from the external network. They form the interface to other parts of the LAN or to the Internet. If the transition to the Internet takes place here, the IP addresses are usually designated by the Internet Service Provider (ISP). If the mGuard is assigned an IP address dynamically, you can look up the currently valid IP address here.

In *Stealth* mode, mGuard adopts the address of the connected local computer as its external IP.

#### Network Mode Status

Displays the status of the selected network mode.

#### Active Defaultroute

Display only: The IP address that the mGuard uses to try to reach unknown networks is displayed here. “(none)” may be shown here in particular if the mGuard is in *Stealth* mode.

#### Used DNS servers

Display only: The name of the DNS servers used by the mGuard for the name resolution are displayed here. This information can be useful, for example, if the mGuard is using the DNS servers designated to it by the Internet Service Provider.

### Network Mode: **Stealth / Router / PPPoE / PPTP / Modem\* / Built-in Modem\***

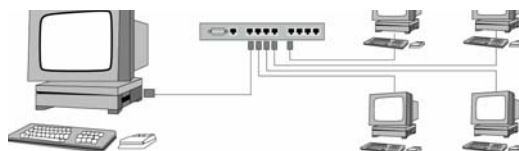
\* *Modem / Built-in Modem*: Not available with all mGuard models – see “Network → Interfaces” on page 105.

The mGuard has to be set to the network mode that corresponds to its connection to the network. See also “Typical Application Scenarios” on page 13.

☞ Depending on which network mode the mGuard is set to, the page will change together with its configuration parameters.

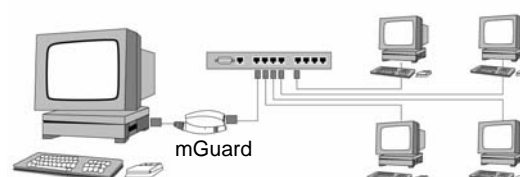
- **Stealth** (*factory default except mGuard delta and blade controller*)  
*Stealth* mode is used to protect a single computer or local network with the mGuard. Important: If the mGuard is in the *Stealth* network mode, it is inserted into the existing network (see illustration) without changing the existing network configuration of the connected devices.

Before



After

(A LAN can also be on the left.)



The mGuard will analyze the network traffic passing through it and configure its network connection accordingly. It will then operate transparently, i.e. without client reconfiguration.

As in the other modes, firewall, anti-virus and VPN security functions are available.

Externally delivered DHCP data is passed through to the connected client.

- ☞ If the mGuard provides services such as VPN, DNS, NTP etc. then a firewall installed on the client must be configured to allow ICMP Echo Requests (ping).
- ☞ In *Stealth* mode the mGuard uses 1.1.1.1 as its internal IP address. This is accessible when the configured default gateway of the client is also accessible.

In the *Stealth* network mode, a secondary external interface can also be configured – see “Secondary external interface (= External 2)” on page 110.

For the further configuration of the *Stealth* network mode, see “→ Network Mode: Stealth” on page 115.

- **Router** (*factory default for mGuard delta and blade controller*)

If the mGuard is in *Router* mode, it serves as a gateway between different networks and has both an external interface (WAN port) and an internal interface (LAN port) with at least one IP address.

#### WAN Port

The mGuard is connected to the Internet or other external parts of the LAN over the WAN port.

- mGuard smart: The WAN port is the ethernet socket.

#### LAN Port

The mGuard is connected to a local network or a single computer over the LAN port.

- mGuard smart: The LAN port is the ethernet connector.
- mGuard PCI:  
In *Driver* mode the LAN port is represented by the network interface of the operating system that has the network card operating system (in this example, the mGuard PCI).  
In *Power-over-PCI* mode the LAN port is the LAN socket of the mGuard PCI.

As in the other modes, firewall, anti-virus and VPN security functions are available.

- ☞ If the mGuard is operated in *Router* mode, it must be set as the standard gateway in the connected local client computers. In other words, the address entered for the standard gateway must be entered as the IP address of the mGuard LAN port.
- ☞ NAT should be activated if the mGuard is operated in *Router* mode and establishes the connection to the Internet. Only then can the computers in the connected local network access the Internet over mGuard – see “Network Security → NAT” on page 172. If NAT is not activated, then only VPN connections can be used.

In the *Router* network mode, a secondary external interface can also be configured – see “Secondary external interface (= External 2)” on page 110. For the further configuration of the *Router* network mode, see “→ Network Mode: Router” on page 118.

- **PPPoE**

*PPPoE* mode corresponds to the Router mode with DHCP – with one difference: The PPPoE protocol, which is used by many DSL modems for DSL Internet access, is used for connecting to the external network (Internet or WAN). The external IP address that the mGuard uses for access from a remote peer is assigned by the Internet Service Provider.

☞ If the mGuard is operated in *PPPoE* mode, it must be set as the standard gateway in the connected local client computers. In other words, the address entered for the standard gateway must be entered as the IP address of the mGuard LAN port.

☞ If the mGuard is operated in *PPPoE* mode, NAT must be activated in order to gain access to the Internet – see “Network Security → NAT” on page 172. If NAT is not activated, then only VPN connections may be used.

For the further configuration of the *PPPoE* network mode, see “→ Network Mode: PPPoE” on page 120.

- **PPTP**

Similar to the *PPPoE* mode. In Austria, for example, PPTP is used instead of the PPPoE protocol for DSL connections.

PPTP is the protocol that was originally used by Microsoft for VPN connections.

☞ If the mGuard is operated in *PPTP* mode, it must be set as the standard gateway in the connected local client computers. In other words, the IP address of the mGuard LAN port must be entered as the standard gateway.

☞ If the mGuard is operated in *PPTP* mode, NAT should be activated in order to gain access to the Internet from the local network – see “Network Security → NAT” on page 172. If NAT is not activated, then only VPN connections can be used.

For the further configuration of the *PPTP* network mode, see “→ Network Mode: PPTP” on page 121.

---

Only *mGuard industrial RS*, *mGuard blade*, *EAGLE mGuard*, *mGuard delta*

---

- **Modem**

Only *mGuard industrial RS* without a built-in modem, *mGuard blade*, *EAGLE mGuard*, *mGuard delta*

If the *Modem* network mode is selected, the external ethernet interface of the mGuard is deactivated and data transfer to and from the WAN is made over the serial mGuard port with external access. An external modem that establishes the connection to the telephone network is connected to the serial port. Internet connection is then made over the telephone network using the external modem.

- ☒ The device reboots automatically when the network mode is changed to or from *Stealth* mode.
- ☒ If the address of the mGuard is changed (e.g. by changing the network mode from *Stealth* to *Router*), the device is only accessible under the new address. When the change is made over the LAN port, a message is displayed with the new address before the change becomes active. When the configuration is changed over the WAN port you will not receive feedback from the mGuard.
- ☒ If you set the mode to *Router*, *PPPoE* or *PPTP* and then change the IP address of the LAN port and/or the local netmask, make sure you enter the correct values. Otherwise, the mGuard may no longer be accessible.

For the further configuration of the *Built-in Modem / Modem* network mode, see “→ Network Mode: Modem / Built-in Modem” on page 122.

---

Only used for *mGuard industrial RS* with built-in modem or ISDN terminal adaptor

---

- **Built-in Modem**

Only used for *mGuard industrial RS* with built-in modem or ISDN terminal adaptor

If the *Built-in Modem* network mode is selected, the external ethernet interface of the mGuard is deactivated and data transfer to and from the WAN is made over the modem or ISDN terminal adaptor installed in the mGuard. This must be connected to the telephone network. Internet connection is then made over the telephone network.

After *Built-in Modem* is selected, the text fields used for the definition of modem connection parameters are displayed.

For the further configuration of the *Built-in Modem / Modem* network mode, see “→ Network Mode: Modem / Built-in Modem” on page 122.

## Secondary external interface (= External 2)

Only for  
*mGuard industrial RS,*  
*mGuard blade,*  
*EAGLE mGuard,*  
*mGuard delta*

➔ Only for ***Stealth*** or ***Router network mode***.

Only for *mGuard industrial RS*, *mGuard blade*, *EAGLE mGuard*, *mGuard delta*:

In these network modes, the serial port of the mGuard can be configured as an additional **secondary external interface**.

The secondary external interface can be used to transfer data *permanently* or *temporarily* into the external network (WAN).

☞ If the serial port of the mGuard is configured as a secondary external interface, then it is not available for dial-in or configuration purposes – see “Modem / Console” on page 133.

### Network mode: Off / Modem / Built-in Modem

#### Off

(Default). Select this setting if the operating environment of the mGuard does not require a secondary external interface. Then you can use the serial port (or the built-in modem, if there is one) for other purposes – see “Modem / Console” on page 133.

#### Modem / Built-in Modem

If you select one of these options, the secondary external interface will be used to transfer data *permanently* or *temporarily* into the external network (WAN).

#### Modem:

The secondary external interface is formed by the serial port of the mGuard and an external modem connected to it.

**Built-in Modem** (only for *mGuard industrial RS* with built-in modem / ISDN terminal adaptor):

The secondary external interface is formed by the built-in modem / the built-in ISDN modem (ISDN terminal adaptor).

- ☞ You enter settings for the modem connection on the **Dial-out** tab page (see Page 126). Under *Dial-out* you also specify whether the telephone connection should be on a dial on demand basis to the remote peer, or permanently as a dedicated line.
- ☞ You enter the connection settings for an external modem on the **Modem / Console** tab page (see Page 133).

**Operation mode: permanent / temporary**

After selecting the *Modem* or *Built-in Modem* network mode for the secondary external interface, you must specify the operation mode of the secondary external interface.

Secondary External Interface					
Network Mode	Modem				
Operation Mode	permanent				
Secondary External Routes	<table border="1"> <thead> <tr> <th>Network</th> <th>Gateway</th> </tr> </thead> <tbody> <tr> <td>192.168.3.0/24</td> <td>%gateway</td> </tr> </tbody> </table>	Network	Gateway	192.168.3.0/24	%gateway
Network	Gateway				
192.168.3.0/24	%gateway				

In both the **permanent** and **temporary** operation modes, the modem must be available to the mGuard for the secondary external interface so that the mGuard can make a connection to the WAN (Internet) over the telephone network connected to the modem.

**permanent / temporary**

Which data packets are transferred over the primary external interface (ethernet interface) and which are transferred over the secondary external interface is determined by the routing settings in effect for these two external interfaces. Therefore an interface can only take a data packet if the routing setting for that interface matches the destination of the data packet.

- **The following rules apply to the use of routing entries.**

- If multiple routing entries match the destination of a packet, then the smallest network defined in the routing entries that match the data packet, decides which route this packet takes.

Example:

The external route of the primary external interface is entered as 10.0.0.0/8, while the external route of the secondary external interface is entered as 10.1.7.0/24. Then data packets to network 10.1.7.0/24 are routed over the secondary external interface, although the routing entry for the primary external interface also matches them. Reason:

The routing entry for the secondary external interface indicates a smaller network (10.1.7.0/24 < 10.0.0.0/8).

- If the routing entries for the primary and secondary external interfaces are identical, then the secondary external interface “wins”, i. e. the data packets with a matching destination address are routed over the secondary external interface.
- The routing settings for the secondary external interface only become effective when the secondary external interface is activated. Particular attention must be paid to this if the routing entries for the primary and secondary external interfaces overlap or are identical, whereby the priority of the secondary external interface has a filter effect, with the following result: Data packets whose destination matches both the primary and secondary external interfaces are always transferred over the secondary external interface, but only if this is activated.

In the **temporary** operation mode, “activated” signifies the following: Only when certain conditions are fulfilled is the secondary external interface activated, and only then do the routing settings of the secondary external interface become effective.

- Network address 0.0.0.0/0 generally signifies the largest definable network, i.e. the Internet.

**permanent**

Data packets whose destination corresponds to the routing settings defined for the secondary external interface are always routed over this external interface. The secondary external interface is always activated.

**temporary**

Data packets whose destination corresponds to the routing settings defined for the secondary external interface are only routed over this external interface when additional conditions to be defined are fulfilled. Only then is the secondary external interface activated, and the routing settings for the secondary external interface become effective – see below:

*Probes for Activation.*

**Secondary external routes****Network**

Here you make the entries for the routing to the external network. You can make multiple routing entries. Data packets intended for these networks are then routed to the corresponding network over the secondary external interface – in *permanent* or *temporary* mode.

**Gateway**

Here you enter the IP address of the gateway over which the transfer is made in the above-named external network – if this IP address is known.

When you are dialing in to the Internet using the phone number of the ISP, the address of the gateway is usually only known after the dial-in. In this case, you enter **%gateway** in the field as a placeholder.

**Probes for Activation**

Secondary External Interface											
Network Mode	Modem										
Operation Mode	temporary										
Secondary External Routes	<table border="1"> <thead> <tr> <th></th> <th>Network</th> <th>Gateway</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td>192.168.3.0/24</td> <td>%gateway</td> </tr> </tbody> </table>				Network	Gateway	<input type="checkbox"/>	192.168.3.0/24	%gateway		
	Network	Gateway									
<input type="checkbox"/>	192.168.3.0/24	%gateway									
Probes for Activation (The secondary external interface is activated only if <i>all</i> probes fail, and if the operation mode is set to "temporary".)	<table border="1"> <thead> <tr> <th></th> <th>Type</th> <th>Destination</th> <th>Comment</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td>ICMP Ping</td> <td>141.1.1.1</td> <td></td> </tr> </tbody> </table>				Type	Destination	Comment	<input type="checkbox"/>	ICMP Ping	141.1.1.1	
	Type	Destination	Comment								
<input type="checkbox"/>	ICMP Ping	141.1.1.1									
Probe Interval (seconds)	20										
Number of times all probes need to fail during subsequent runs before the secondary external interface is activated.	2										
DNS Mode	use primary DNS settings untouched										
User defined name servers (If they should be reachable via the secondary external interface please configure a route for them.)	<table border="1"> <thead> <tr> <th></th> <th>IP</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td>198.41.0.4</td> </tr> </tbody> </table>				IP	<input type="checkbox"/>	198.41.0.4				
	IP										
<input type="checkbox"/>	198.41.0.4										

If the operation mode of the secondary external interface is set to **temporary**, then the following is checked using periodic ping probes: Can a particular destination or destinations be reached when data packets take the route based on all the routing settings defined for the mGuard – apart from those defined for the secondary external interface? Only if none of the ping probes is successful does the mGuard assume that it is currently not possible to reach the destination(s) over the primary external interface (= ethernet interface over WAN port of the mGuard). It is only in this case that the secondary external interface activated, which results in the data packets being routed over this interface – if the corresponding routing settings are made for the secondary external interface.

The secondary external interface remains activated until the mGuard detects in subsequent ping probes that the destination(s) can be reached again. When this condition is fulfilled, the data packets are routed over the primary external interface again and the secondary external interface is deactivated.

Therefore the purpose of the ongoing ping probes is to check whether specific destinations can be reached over the primary external interface. When they cannot be reached, the secondary external interface is activated until they can be reached again.

**Type / Destination**

Specify the ping **Type** for the ping request packet that the mGuard will send to the device with the IP address that you enter under **Destination**.

You can configure multiple ping probes for different destinations.

**Success / failure:**

A ping probe is successful if the mGuard receives a positive response to the outgoing ping request packet within 4 seconds. If the response is positive, the remote peer can be reached.

**Ping types:****IKE Ping:**

Determines whether a VPN gateway can be reached at the IP address entered.

**ICMP Ping:**

Determines whether a device can be reached at the IP address entered.

This is the most common ping probe. However, the response to this ping probe is switched off on some devices, so that they do not respond even though they can be reached.

**DNS Ping:**

Determines whether a functioning DNS server can be reached at the IP address entered.

A generic request is sent to the DNS server with the specified IP address, and every DNS server that can be reached responds to this request.

Please note the following when programming ping probes:

It makes sense to program multiple ping probes. This is because it is possible that an individual probed service is currently undergoing maintenance. In such a case, the result should not be that a secondary external interface is activated and a cost-incurring dial connection over the telephone network is set up.

Because the ping probes generate network traffic, the number of probes and their frequency should be kept within reasonable limits. You also want to avoid activating the secondary external interface too early. The timeout period for the individual ping requests is 4 seconds. This means that after a ping probe is started, the next ping probe starts after 4 seconds if the previous one was negative.

To take this aspect into account, you make the following settings.

**Probe Interval (seconds)**

The ping probes defined above under **Probes for Activation** are performed one after the other. When the ping probes defined are performed once in sequence, this is known as a *probe run*. Probe runs are performed continuously at intervals. The interval entered in this field specifies how long the mGuard waits after starting a probe run before it starts the next probe run. The probe runs are not necessarily performed to completion: As soon as one ping probe in a probe run is successful, the subsequent ping probes in this probe run are omitted. If a probe run takes longer than the interval specified, then the subsequent probe run is started directly after it.

**Number of times all probes need to fail during subsequent runs before the secondary external interface is activated**

Specifies how many sequentially performed probe runs must return a negative result before the mGuard activates the secondary external interface. The result of a probe run is negative if none of the ping probes it contains was successful.

The number specified here also indicates how many consecutive probe runs must be successful after the secondary external interface has been activated, before this interface is deactivated again.

**DNS Mode**

Only relevant if the secondary external interface is activated in the **temporary** operation mode:

The DNS mode selected here specifies which DNS server the mGuard uses for temporary connections set up over the secondary external interface.

Possible settings:

- Use primary DNS settings untouched
- DNS Root Servers
- Provider defined (via PPP dial-up)
- User defined (servers listed below)

**Use primary DNS settings untouched**

The DNS server(s) defined under Network --> DNS Server (see “Network → DNS” on page 139) is used.

**DNS Root Servers**

Queries are sent to the root servers in the Internet whose IP addresses are stored in the mGuard. These addresses rarely change.

**Provider defined (via PPP dial-up)**

The domain name servers of the Internet Service Provider that provides access to the Internet are used.

**User defined (servers listed below)**

If this setting is selected, the mGuard will connect to the domain name servers shown in the subsequent list of *User defined name servers*.

**User defined name servers**

You can enter the IP addresses of domain name servers in this list.

The mGuard uses this list for communication over the secondary external interface – as long as the interface is activated temporarily and the **DNS mode** (see above) is specified as *user defined* for this case.

## → Network Mode: Stealth

(Factory default except mGuard delta and blade controller)

When "Stealth" network mode and "static" stealth configuration are set

The screenshot shows the 'Network > Interfaces' configuration page. The 'General' tab is selected. Under 'Network Status', the 'External IP address' is set to 'Primary: 192.168.66.1' and 'Secondary: (not in use)'. The 'Active Default route' is '(none)' and 'Used DNS servers' are 'DNS Root Servers'. Under 'Network Mode', 'Network Mode' is set to 'Stealth' and 'Stealth configuration' is set to 'static'. Under 'Stealth Management IP Address', there is a note: 'Here you can specify an additional IP address to administrate the mGuard. If you have set "Stealth configuration" to "multiple clients", remote access will only be possible using this IP address. An IP address of "0.0.0.0" disables this feature. Note: using management VLAN is not supported in Stealth autodetect mode.' The fields are: IP address (0.0.0.0), Netmask (0.0.0.0), Default gateway (0.0.0.0), Use Management VLAN (No), and Management VLAN ID (1). Under 'Static routes', there is a note: 'The following settings are applied to traffic generated by the mGuard. Networks to be routed over alternative gateways'. A table with columns 'Network' and 'Gateway' is shown. Under 'Static Stealth Configuration', the fields are: Client's IP address (0.0.0.0) and Client's MAC address (0:0:0:0:0:0). Under 'Secondary External Interface', 'Network Mode' is set to 'Off'.

### Stealth configuration: autodetect / static / multiple clients

#### autodetect

(Default) The mGuard analyzes the network traffic and independently configures its network interface accordingly. It functions transparently.

#### static

If the mGuard cannot analyze the network traffic (e.g. because the connected local computer only receives data), then the *Stealth configuration* must be set to **static**. In this case, further text fields are provided for the static stealth configuration.

#### multiple clients

As with **autodetect**, but it is possible to connect more than one computer to the mGuard LAN port (secure port), meaning that several IP addresses can be used here.

### Stealth Management IP Address

#### Stealth Management IP Address

Here you can specify an additional IP address to administrate the mGuard. If you have set "Stealth configuration" to "multiple clients", remote access will only be possible using this IP address. An IP address of "0.0.0.0" disables this feature. Note: using management VLAN is not supported in Stealth autodetect mode.

IP address	10.1.66.253
Netmask	255.255.0.0
Default gateway	10.1.0.254
Use Management VLAN	No
Management VLAN ID	1

An additional IP address can be specified here to administrate the mGuard.

Remote access via HTTPS, SNMP and SSH is only possible using this address if:

- *Stealth configuration* is set to the option **multiple clients**
- The client does not answer ARP requests
- No client is available

☒ In the *static* stealth configuration, the *Stealth management IP address* is always accessible, even when the network card of the client PC is not activated.

**IP address**

The additional IP address for contact and administration of the mGuard.  
The IP address “0.0.0.0” disables the management IP address.

**Netmask**

The netmask for the IP address above.

**Default gateway**

The default gateway (standard gateway) of the network where the mGuard is located.

**Use Management VLAN: Yes / No**

If this IP address should be contained within a VLAN, then this option must be set to **Yes**.

**Management VLAN ID**

A VLAN ID between 1 and 4095.

☒ VLAN is not supported for the management IP address during *automatic* stealth configuration.

 An explanation of the term “VLAN” can be found in the glossary under Page 261.

**Static routes** (Stealth configuration = static)




In *Stealth* mode the mGuard adopts the default gateway of the client connected to the LAN port. Alternative routes can be defined for data packets in WAN created by the mGuard. Among others, the following data traffic packets belong here:

- The download of certificate revocation lists (CRL)
- The download of a new configuration or virus definition file
- Communication with an NTP server (for time synchronization)
- Dispatch and receipt of encrypted data packages from VPN connections
- Queries to DNS servers
- Syslog messages
- The download of firmware updates
- The download of configuration profiles from a central server (if configured)
- SNMP traps

If this option is used, make the relevant entries afterwards. If it is not used, the affected data packages are transmitted over the default gateway defined by the client.

**Static routes**

*The following settings are applied to traffic generated by the mGuard.*

Networks to be routed over alternative gateways		Network	Gateway
			
		192.168.101.0/24	10.1.0.253

**Network**

Enter the network using CIDR notation – see “CIDR (Classless Inter-Domain Routing)” on page 246.

**Gateway**

The gateway where this network can be accessed.

The routes defined here are valid as necessary routes for data packages created by the mGuard. This definition takes priority over other settings.

 See also “Network Example” on page 247.

## Stealth Static Stealth Configuration

### Client IP address

The IP address of the client connected to the LAN port.

### Client MAC address

The physical address of the network adaptor in the local computer where the mGuard is connected.



The MAC address can be determined as follows:

On the DOS level (Start, Programs, Accessories, Command Prompt), enter the following command:

**ipconfig /all**

The entry of a MAC address is not necessary. The mGuard can obtain the MAC address automatically from the client. The MAC address 0:0:0:0:0:0 must be entered in order to do this. Please note that the mGuard can only forward the network package through to the client after the MAC address has been determined.

If no *Stealth management IP address* or *Client's MAC address* is configured in static Stealth mode, then DAD ARP requests are sent to the internal interface (see RFC2131, section 4.4.1).

## → Network Mode: Router

(Factory default for mGuard delta and blade controller)

When the “Router” network mode is selected

**Network >> Interfaces**

General | Ethernet | Dial-out | Dial-in | Modem / Console

**Network Status**

External IP address	Primary: 192.168.66.1 Secondary: (not in use)
Active Defaultroute	(none)
Used DNS servers	DNS Root Servers

**Network Mode**

Network Mode: Router

**External Networks**

Obtain external configuration via DHCP: No

External IPs (untrusted port)	IP	Netmask	Use VLAN	VLAN ID
	10.0.0.152	255.255.255.0	No	1

Additional External Routes

Network	Gateway

IP of default gateway: 10.0.0.253

**Internal Networks**

Internal IPs (trusted port)	IP	Netmask	Use VLAN	VLAN ID
	192.168.1.1	255.255.255.0	No	1

Additional Internal Routes

Network	Gateway

### External Networks (Network Mode = Router)

#### Obtain external configuration via DHCP: Yes / No

- ☞ If the mGuard obtains configuration data via DHCP (Dynamic Host Configuration Protocol) from the DHCP server, enter **Yes** here. In this case, all other entries made under **External Networks** have no effect. The related fields on the page are then hidden.
- ☞ If the mGuard does not obtain configuration data via DHCP (Dynamic Host Configuration Protocol) from the DHCP server, enter **No** and make the following additional entries:

#### External IPs (untrusted port)

The addresses on the WAN port side where devices can access the mGuard. If the transition to the Internet takes place here, the external IP of the mGuard is designated by the Internet Service Provider (ISP).

- ☒ Only the first external IP address entered here is used for the handling of VPN connections.

#### IP/Netmask

IP address and netmask of the WAN port.

#### Use VLAN: Yes / No

If this IP address should be contained within a VLAN, then this option must be set to **Yes**.

#### VLAN ID

A VLAN ID between 1 and 4095.

- ☞ An explanation of the term “VLAN” can be found on Page 261.
- ☞ If you want to delete entries from the list, please note that the first entry cannot be deleted.

**Additional External Routes**

In addition to the default route over the default (standard) gateway (see below), you can define additional external routes.

**Network / Gateway**

See also “Network Example” on page 247.

**IP of default gateway**

The IP address of a device in the local network (connected to the LAN port) or the external network (connected to the WAN port) can be specified here.

If the mGuard establishes the transition to the Internet, this IP address is designated by the Internet Service Provider (ISP). If mGuard is utilized within the LAN, the IP address of the default gateway is designated by the network administrator.

- ☒ If the local network is not known to the external router (e.g. in case of configuration by DHCP), enter the address of your local network under Network Security → NAT (see “Network Security → NAT” on page 172).

**Internal Networks**

Configuration of the internal network is described under “Network Mode → Router, PPPoE, PPTP or Modem / Built-in Modem” on page 123.

## → Network Mode: PPPoE

When the “PPPoE”  
network mode is  
selected

**Network >> Interfaces**

General | Ethernet | Dial-out | Dial-in | Modem / Console

**Network Status**

External IP address: Primary: 192.168.66.1  
Secondary: (not in use)

Active Default route: (none)

Used DNS servers: DNS Root Servers

**Network Mode**

Network Mode: PPPoE

**PPPoE**

PPPoE Login: user@provider.example.net

PPPoE Password:

Automatic Re-connect?: No

Re-connect daily at: 0 h 0 m

**Internal Networks**

	IP	Netmask	Use VLAN	VLAN ID
Internal IPs (trusted port)	192.168.1.1	255.255.255.0	No	1

**Additional Internal Routes**

Network	Gateway

## PPPoE

For access to the Internet, the Internet Service Provider (ISP) gives the user a login name and password. These are required for connection to the Internet.

### PPPoE Login

The user name (Login) that is required by your Internet Service Provider (ISP) when you setup a connection to the Internet.

### PPPoE Password

The password that is required by your ISP when you setup a connection to the Internet.

### Automatic Re-connect? Yes / No

Enter the time in the **Re-connect daily at** field next to **Yes**. This feature is used to schedule Internet disconnection and reconnection (as required by many ISPs) so that they do not interrupt normal business operations.

When this function is activated, it only comes into action when synchronization with a time server has been made – see “Management → System Settings”, “Time and Date” on page 62.

### Re-connect daily at

Time when *Automatic Re-connect* (see above) takes place.

## Internal Networks

Configuration of the internal network is described under “Network Mode → Router, PPPoE, PPTP or Modem / Built-in Modem” on page 123.

## → Network Mode: PPTP

When the "PPTP"  
network mode is  
selected

Network > Interfaces				
General   Ethernet   Dial-out   Dial-in   Modem / Console				
<b>Network Status</b>				
External IP address	Primary: 192.168.66.1 Secondary: (not in use)			
Active Defaultroute	(none)			
Used DNS servers	DNS Root Servers			
<b>Network Mode</b>				
Network Mode	PPTP			
<b>PPTP</b>				
PPTP Login	user@provider.example.net			
PPTP Password				
Local IP Mode	Static (from field below)			
Local IP	10.0.0.140			
Modem IP	10.0.0.138			
<b>Internal Networks</b>				
Internal IPs (trusted port)	IP	Netmask	Use VLAN	VLAN ID
	192.168.1.1	255.255.255.0	No	1
Additional Internal Routes	Network		Gateway	

### PPTP

For access to the Internet, the Internet Service Provider (ISP) gives the user a login name and password. These are required for connection to the Internet.

#### PPTP Login

The user name (Login) that is required by your Internet Service Provider when you setup a connection to the Internet.

#### PPTP Password

The password that is required by your ISP when you setup a connection to the Internet.

#### Local IP Mode: Static / Via DHCP

##### Via DHCP:

If the address data for access to the PPTP server is supplied by the Internet Service Provider via DHCP, select **Via DHCP**.

You then do not need to make an entry in the **Local IP** field.

##### Static (from field below):

If the address data for access to the PPTP server is not supplied by the Internet Service Provider via DHCP, then the local IP address must be entered.

#### Local IP

The IP address where the mGuard can be accessed by the PPTP server.

#### Modem IP

The address of the PPTP server at the Internet Service Provider.

#### Internal Networks

Configuration of the internal network is described under "Network Mode → Router, PPPoE, PPTP or Modem / Built-in Modem" on page 123.

## → Network Mode: Modem / Built-in Modem

Only *mGuard industrial RS*, *mGuard blade*, *EAGLE mGuard*, *mGuard*, *mGuard delta*

→ The **Modem** network mode is available for:

*mGuard industrial RS*, *mGuard blade*, *EAGLE mGuard*, *mGuard delta*.

→ The **Built-in Modem** network mode is additionally available for:

*mGuard industrial RS*, if this has a built-in modem or ISDN terminal adaptor (optional).

In all of the devices mentioned above, data traffic is transferred over the internal serial port and not over the mGuard WAN port when the *Modem* or *Built-in Modem* network mode is activated. From there it is either:

A – Transferred over the external serial port where an external modem must be connected

OR

B – Transferred over the built-in modem or ISDN terminal adaptor (for mGuard industrial RS, when equipped)

In both cases the connection to the ISP and Internet is established over the telephone network using a modem or ISDN terminal adaptor.

☞ In the *Modem* network mode, the serial port of the mGuard is not available for the PPP dialin option or for configuration purposes – see “Modem / Console” on page 133.

The screenshot shows the 'Network >> Interfaces' configuration window with the 'Modem / Console' tab selected. The 'Network Status' section shows 'External IP address' with 'Primary: 192.168.66.1' and 'Secondary: (not in use)', 'Active Defaultroute' as '(none)', and 'Used DNS servers' as 'DNS Root Servers'. The 'Network Mode' is set to 'Modem'. The 'Internal Networks' section contains a table for 'Internal IPs (trusted port)' with columns for IP, Netmask, Use VLAN, and VLAN ID. The first entry has IP '192.168.1.1', Netmask '255.255.255.0', 'No' for Use VLAN, and '1' for VLAN ID. Below this is a section for 'Additional Internal Routes' with columns for 'Network' and 'Gateway'.

Network >> Interfaces				
General   Ethernet   Dial-out   Dial-in   <b>Modem / Console</b>				
<b>Network Status</b>				
External IP address	Primary: 192.168.66.1 Secondary: (not in use)			
Active Defaultroute	(none)			
Used DNS servers	DNS Root Servers			
<b>Network Mode</b>				
Network Mode	Modem			
<b>Internal Networks</b>				
Internal IPs (trusted port)	IP	Netmask	Use VLAN	VLAN ID
	192.168.1.1	255.255.255.0	No	1
Additional Internal Routes	Network		Gateway	

After selecting the **Modem** network mode, you enter the required parameters for the modem connection on the **Dial-out** and/or **Dial-in** tab pages. See “Dial-out” on page 126 and “Dial-in” on page 130.

You enter the connection settings for an external modem on the **Modem / Console** tab page. See “Modem / Console” on page 133.

\* Also **Built-in Modem** for the mGuard industrial RS (only available as an option for the mGuard industrial RS with built-in modem / ISDN terminal adaptor).

Configuration of the internal network is described in the next section.

**Network Mode →  
Router, PPPoE,  
PPTP or Modem /  
Built-in Modem**

### **Internal Networks**

#### **Internal IPs (trusted port)**

The internal IP is the IP address where the mGuard can be accessed by devices on the locally connected network.

The factory defaults for **Router/PPPoE/PPTP/Modem** mode are as follows:

IP address:	<b>192.168.1.1</b>
Local netmask:	<b>255.255.255.0</b>

You can also specify other addresses where the mGuard can be accessed by devices on the locally connected network. For example, this can be useful if the locally connected network is divided into subnetworks. Multiple devices on different subnetworks can then access the mGuard under different addresses.

#### **IP**

IP address where the mGuard is accessible over the LAN port.

#### **Netmask**

The netmask of the network connected to the LAN port.

#### **Use VLAN**

If this IP address should be contained within a VLAN, then this option must be set to **Yes**.

#### **VLAN ID**

A VLAN ID between 1 and 4095.



An explanation of the term “VLAN” can be found in the glossary under Page 261.



If you want to delete entries from the list, please note that the first entry cannot be deleted.

### **Additional Internal Routes**

Additional routes can be defined if further subnetworks are connected to the local network.

#### **Network**

Enter the network using CIDR notation – see “CIDR (Classless Inter-Domain Routing)” on page 246.

#### **Gateway**

The gateway where this network can be accessed.



See also “Network Example” on page 247.

Ethernet

Network > Interfaces

General

Ethernet

Dial-out

Dial-in

Modem / Console

ARP Timeout

ARP Timeout

30

MTU Settings

MTU of the internal interface

1500

MTU of the internal interface for VLAN

1500

MTU of the external interface

1500

MTU of the external interface for VLAN

1500

MTU of the Management Interface

1500

MTU of the Management Interface for VLAN

1500

MAU Configuration

Port	Media Type	Link State	Automatic Configuration	Manual Configuration	Current Mode	Port On
External	10/100 BASE-T/RJ45	down	Yes	100 Mbit/s FDX	-	Yes
Internal	10/100 BASE-T/RJ45	up	Yes	100 Mbit/s FDX	100 Mbit/s FDX	Yes

ARP Timeout

ARP Timeout

Lifetime of entries in the ARP table (in seconds).

MTU Settings

MTU of the <name> interface

The Maximum Transfer Unit (MTU) defines the maximum IP packet length allowed for using the respective interface.

☒ For VLAN interfaces:

As VLAN packages contain 4 bytes more than those without VLAN, certain drivers may have problems in processing larger packets. Such problems can be solved by reducing the MTU to 1496.

Configuration and status display of the ethernet ports:

MAU Configuration

Port

Name of the ethernet port that the row refers to.

Media Type

Media type of the ethernet port.

Link State

**Up:** Connection is made.

**Down:** Connection is not made.

Automatic Configuration: Yes / No

**Yes:** Tries to determine the required operating mode automatically.

**No:** Uses the operating mode specified in the “Manual Configuration” column.

☒ When connecting the mGuard industrial RS or EAGLE mGuard to a hub, please note the following: When *Automatic Configuration* is deactivated, the Auto MDIX function is also deactivated. This means that the mGuard industrial RS or EAGLE mGuard port must either be connected to the uplink port of the hub or be connected using a cross-link cable.

**Manual Configuration**

The desired operating mode when *Automatic Configuration* is set to *No*.

**Current Mode**

Current network connection mode.

**Port On: Yes / No (only *mGuard industrial RS*, *EAGLE mGuard* and *mGuard smart*)**

Enables/disables the ethernet port.

## Dial-out

Only *mGuard industrial RS*, *mGuard blade*, *EAGLE mGuard*, *mGuard delta*

- ➔ Is only configured if the mGuard is to be able to make a data connection (dial-out) to the WAN (Internet)
- over the primary external interface (*Modem* or *Built-in Modem* network mode)
- OR
- over the secondary external interface (also available in the *Stealth* or *Router* network mode)

### PPP options (dial-out)

#### Phone number to call

Telephone number of the ISP. The connection to the Internet is established after telephone connection is made.

Command syntax

Together with the previously set modem command for dialing ATD, the following dial sequence (as an example) is created for the connected modem: **ATD765432**

A compatible pulse dialing procedure is used as standard which works correctly in all cases.

Special dial characters can be used in the dial sequence. See the following table for more details:

HAYES special dial characters:

- W** Instructs the modem to make a pause in dialing until the dial tone can be heard.  
Used when the modem is connected to a private branch exchange. An external line must be obtained first for outgoing calls by dialing a certain number (e.g. 0) before the desired telephone number can be dialed. Example: **ATD0W765432**
- T** Change to tone dialing  
Set the special dial character **T** before the dialed number if the faster tone dialing procedure should be used (only with tone-compatible telephone connections). Example: **ATDT765432**

#### Authentication: PAP / CHAP / None

PAP = Password Authentication Protocol, CHAP = Challenge Handshake Authentication Protocol. These are procedures used for the secure transfer of authentication data over Point-to-Point Protocol.

If the ISP requires the user to login using user name and password, then PAP or CHAP is used as the authentication procedure. The user name, password and any other entries needed for the user to access the Internet are given to the user by the ISP.

The relevant fields are displayed depending on whether **PAP**, **CHAP** or **None** is selected. Enter the relevant data in these fields.

### If authentication is made via PAP:

Authentication	PAP ▼
User name	<input type="text"/>
Password	<input type="password"/>
PAP server authentication	No ▼
Dial on demand	Yes ▼
Idle timeout	Yes ▼
Idle time (seconds)	300
Local IP	0.0.0.0
Remote IP	0.0.0.0
Netmask	0.0.0.0

#### User name

User name entered during ISP login to access the Internet.

#### Password

Password entered during ISP login to access the Internet.

#### PAP server authentication: Yes / No

##### Yes:

The following two fields appear:

##### Server user name

##### Server password

User name and password that the mGuard queries from the server. mGuard only allows the connection when the server provides the agreed user name and password combination.

#### Subsequent fields

See under “If “None” is selected as authentication” on page 128.

### If authentication is made via CHAP:

Authentication	CHAP ▼
Local name	<input type="text"/>
Remote name	<input type="text"/>
Secret for client authentication	<input type="password"/>
CHAP server authentication	No ▼
Dial on demand	Yes ▼
Idle timeout	Yes ▼
Idle time (seconds)	300
Local IP	0.0.0.0
Remote IP	0.0.0.0
Netmask	0.0.0.0

#### Local name

A name used by the mGuard at the ISP. The service provider may have several customers. This name allows the ISP to identify who is dialing. After the mGuard has provided this name, the ISP also checks the *Secret for client authentication* (see below). The connection can only be made successfully when the name is known to the ISP and the password matches.

**Remote peer name**

A name given by the ISP to the mGuard for identification purposes.  
The mGuard will not connect to the service provider when the ISP does not give the correct name.

**Secret for client authentication**

Password entered during ISP login to access the Internet.

**CHAP server authentication: Yes / No****Yes:**

The following entry field appears:

**Password for server authentication**

The password that the mGuard queries from the server. mGuard only allows the connection when the server provides the agreed password.

**Subsequent fields**

See under “If “None” is selected as authentication” on page 128.

**If “None” is selected as authentication**

In this case all fields that relate to PAP or CHAP are hidden.

Only the fields that define further settings remain visible.

Dial on demand	Yes ▾
Idle timeout	Yes ▾
Idle time (seconds)	300
Local IP	0.0.0.0
Remote IP	0.0.0.0
Netmask	0.0.0.0

**Dial on demand: Yes / No**

**Yes** (standard): This setting is useful for telephone connections where costs are calculated according to connection length.

The mGuard only commands the modem to establish a telephone connection when network packages are to be transferred. It also instructs the modem to terminate the telephone connection as soon as no more network packages are to be transferred for a specific time (see values in *Idle timeout*). By doing this, the mGuard is not constantly available externally (i.e. for incoming data packages).

When **No** is selected, the mGuard establishes a telephone connection using a connected modem as soon as possible after a reboot or activation of the *Modem* network mode. This remains in place constantly, regardless of whether data is transferred or not. If the telephone connection is then interrupted, the mGuard attempts to restore it immediately. A constant connection is then made (like a dedicated line). By doing this, the mGuard is constantly available externally (i. e. for incoming data packages).

☒ For both *Yes* and *No*: The telephone connection is always made by the mGuard.

**Idle timeout: Yes / No**

Only considered when *Dial on demand* is set to **Yes**.

When **Yes** (default) is set, the mGuard terminates the telephone connection as soon as no data transfer takes place over the defined idle period. The mGuard gives the connected modem the relevant command for terminating the telephone connection.

When **No** is set, the mGuard gives the connected modem no command for terminating the telephone connection.

**Idle time (seconds)**

Standard: 300. If no data traffic is made after the time specified here, the mGuard can terminate the telephone connection – see above under *Idle timeout*.

**Local IP**

IP address of the mGuard serial port that now acts as a WAN interface. Adopt the preset value if this IP address is assigned dynamically by the ISP: 0.0.0.0

Otherwise enter this here (i.e. assignment of a fixed IP address).

**Remote IP**

IP address of the remote peer. This is the IP address of the ISP used for access when connecting to the Internet. As PPP is used for the connection, the IP address is not normally specified. This means you can use the predefined value: 0.0.0.0

**Netmask**

The netmask here belongs to both *Local* and *Remote* IP addresses.

Normally all three values (*Local IP*, *Remote IP* and *Netmask*) are set, or all remain set to 0.0.0.0.



You enter the connection settings for an external modem on the **Modem / Console** tab page. See “Modem / Console” on page 133.

## Dial-in

Only *mGuard industrial RS*, *mGuard blade*, *EAGLE mGuard*, *mGuard delta*

The screenshot shows the 'Network » Interfaces' configuration page with the 'Dial-in' tab selected. The 'Modem (PPP)' option is set to 'Off'. The 'Local IP' is 192.168.2.1 and the 'Remote IP' is 192.168.2.2. The 'PPP Login name' is 'admin' and the 'PPP Password' is masked with asterisks. Below these fields are sections for 'Incoming Rules (PPP)' and 'Outgoing Rules (PPP)', each with a table for defining rules based on protocol, IP, and port. A note at the bottom states: 'Please note: On some platforms the serial port is not accessible.'

- ➔ Is only configured if the mGuard is to permit PPP dialin over either
- a modem connected to the serial port or
  - a built-in modem (option available with the mGuard industrial RS).

The PPP dialin can be used to access the LAN (or the mGuard for configuration purposes) – see “Modem / Console” on page 133

- ☞ If the modem is used for dialing out by functioning as the primary external interface (*Modem network mode*) of the mGuard or as its secondary external interface (when activated in the *Stealth* or *Router network mode*), then it is not available for the PPP dialin option.

## PPP dialin options

- ➔ For *mGuard industrial RS* (without built-in modem or ISDN TA), *mGuard blade*, *delta* and *EAGLE mGuard*:

**Modem (PPP): Off / On**

The setting must be **Off** if no serial port is to be used for the PPP dialin option.

If it is set to **On**, the PPP dialin option is available. You enter the connection settings for the connected external modem on the **Modem / Console** tab page.

- ➔ For *mGuard industrial RS* (with built-in modem or ISDN TA):

**Modem (PPP): Off / Built-in Modem / External Modem**

The setting must be **Off** if the serial port is not to be used for the PPP dialin option.

If it is set to **External Modem**, the PPP dialin option is available. Then an external modem must be connected to the serial port. You enter the connection settings for the connected external modem on the **Modem / Console** tab page.

If this is set to **Built-in Modem**, the PPP dialin option is available. In this case the modem connection is not made over the *Serial Port* socket on the front side. Instead, it is made over the terminal block on the bottom, where the built-in modem or ISDN terminal adaptor is connected to the telephone network. You enter the connection settings for the built-in modem on the **Modem / Console** tab page.

If you are using the **Built-in Modem** option, you can also use the serial port. For the usage options, see “Modem / Console” on page 133.

**Local IP**

IP of the mGuard that can be accessed by a PPP connection.

**Remote IP**

IP address of the PPP connection remote peer.

**PPP Login name**

Login name that the PPP remote peer has to enter to gain access to the mGuard using PPP.

**PPP Password**

Password that the PPP remote peer has to enter to gain access to the mGuard using PPP.

**Incoming Rules (PPP)**

Firewall rules for PPP connection to the LAN interface.

If multiple firewall rules are set, they will be searched in the order in which they are listed (top-down) until a suitable rule is found. This rule is then applied. If there are other suitable rules further down the list, then these are ignored.

You have the following options:

**Protocol**

**All** means: TCP, UDP, ICMP and other IP protocols.

**From / To IP**

**0.0.0.0/0** means all IP addresses. To enter an address, use CIDR notation – see “CIDR (Classless Inter-Domain Routing)” on page 246.

**From / To Port**

(Only evaluated for TCP and UDP protocols)

**any** describes any selected port.

**startport:endport** (e.g. 110:120) defines a range of ports.

You can specify individual ports by giving either their port number or the corresponding service name: (e.g. 110 for pop3 or pop3 for 110).

**Action**

**Accept** means that data packets may pass through.

**Reject** means that the data packets are rejected. The sender is informed that the data packets have been rejected.

**Drop** means that data packets may not pass through. Data packets are discarded and the sender is not informed of their whereabouts.

**Comment**

Freely selectable comment for this rule.

**Log**

For each individual firewall rule you can specify whether the use of the rule

 should be logged (set *Log* to **Yes**) or

 should not be logged (set *Log* to **No** – factory default)

**Log entries for unknown connection attempts?: Yes / No**

When set to **Yes**, all attempts to establish a connection that are not covered by the rules defined above are logged.

### **Outgoing Rules (Port)**

Firewall rules for PPP connection from the LAN interface.

The parameters correspond to those of the *Incoming Rules (PPP)* – see above.

These outgoing rules apply to data packets that are sent out over a data connection initiated by PPP dialin.

## Modem / Console

Only *mGuard industrial RS*, *mGuard blade*, *EAGLE mGuard*, *mGuard delta*

**Network > Interfaces**

**General** **Ethernet** **Dial-out** **Dial-in** **Modem / Console**

**Serial Console**

Baudrate: 57600

Hardware handshake RTS/CTS: Off

Please note: On some platforms the serial port is not accessible. The settings above become effective only for administrative shell login via a console connected to the serial port. Such logins are impossible if dial-in or dial-out is configured via external modem.

**External Modem**

Hardware handshake RTS/CTS: Off

Baudrate: 57600

Handle modem transparently (for dial-in only): Yes

Modem init string: \*\d+++dATH OK

Some mGuard models have a serial port with external access, while the mGuard industrial RS is also optionally equipped with a built-in modem – see “Network → Interfaces” on page 105.

### Options for using the serial port

Alternatively, the serial port can be used as follows:

- As a primary external interface, if the network mode is set to **Modem** under *Network → Interfaces*, on the *General* tab page – see “Network → Interfaces”, “General” on page 106. In this case, the data traffic is not made over the WAN port (= ethernet port) but over the serial port.

OR

- As a secondary external interface, if the **secondary external interface** is activated and **Modem** is selected under *Network → Interfaces*, on the *General* tab page – see “Network → Interfaces”, “General” on page 106. In this case the data traffic – permanent or temporary – is made over the serial port.

OR

- For dialing in to the LAN or for configuration purposes (see also “Dial-in” on page 130). The following possibilities are available:
  - A Connect a modem to the serial port of the mGuard. This is connected to the telephone network (landline or GSM network). (Connection to the telephone network is made over the terminal block on the bottom of the device for the mGuard industrial RS with built-in modem or ISDN terminal.) This enables a remote PC that is also connected to the telephone network to establish a PPP (Point-to-Point Protocol) dial-up connection to the mGuard via a modem or ISDN adaptor. This procedure is defined as a PPP dialin option. It can be used to access the LAN behind the mGuard or to configure the mGuard. **Dial-in** is the interface definition used for this connection type in firewall selection lists.

For you to be able to access the LAN with a Windows computer using the dial connection with TCP/IP, a network connection must be set up on this computer in which the dial connection to the mGuard is defined. Additionally, the IP address of the mGuard (or its hostname) must be defined as a gateway for this connection so that the connections to the LAN can be routed over this.

To access the web configuration interface of the mGuard, you must enter the IP address of the mGuard (or its hostname) in the address line of the web browser.

- B Connect the serial port of the mGuard to the serial port of a PC. Establish the connection to the mGuard on a PC by using a terminal program and carry out the configuration using the command line interface of the mGuard.

If an external modem is connected to the serial port, you may have to enter corresponding settings below under ***External Modem***, regardless of what you are using the serial port and the modem connected to it for.

### Serial Console

☒ The following settings for the *Baudrate* and the *Hardware handshake* are only valid for configurations where a terminal or PC with a terminal program is connected to the serial port, as described above under “B”. Not valid when an external modem is connected. You enter the settings for this further down under ***External Modem***.

#### Baudrate

You can define the transfer speed of the serial port over the selection list.

#### Hardware handshake RTS/CTS: Off / On

When set to **On**, flow control through RTS and CTS signals is used.

### External Modem

#### Hardware handshake RTS/CTS: Off / On

When set to **On**, flow control through RTS and CTS signals is used during PPP connection.

#### Baudrate

Standard: 57600. Transfer speed for communication between mGuard and modem over the serial cable connection.

This should be set to the highest level supported by the modem. If the value is set lower than the maximum possible for the modem then the telephone connection will not work optimally.

#### Handle modem transparently (for dial-in only): Yes / No

If the external modem is used for dialing in (see “PPP dialin options” on page 130), then a **Yes** setting means that the mGuard does not initialize the modem. The subsequently configured modem initialization sequence is not considered. Thus, either a modem is connected which can answer calls itself (standard profile of the modem contains “auto answer”), or else a null-modem cable to a computer can be used instead of the modem, and the PPP protocol is used over this.

**Modem init string**

The initialization sequence that is sent by the mGuard to the connected modem.

Standard: `'' \d+++ \dATH OK`

If necessary, consult the modem manual for the initialization sequence.

The initialization sequence is a sequence of character strings expected by the modem, and commands, that are then sent to the modem so that the modem can establish a connection.

The preset initialization sequence has the following meaning:

<code>''</code>	(two simple quotation marks placed directly after one another) The empty character string inside the quotation marks means that the mGuard does not initially expect any information from the connected modem, but rather sends the following text directly to the modem.
<code>\d+++ \dATH</code>	The mGuard sends this character string to the modem in order to establish the readiness of the modem for accepting commands.
<code>OK</code>	Specifies that the mGuard expects the <b>OK</b> character string from the modem as an answer to <code>\d+++ \dATH</code> .

☒ With many modem types it is possible to save modem settings in the modem itself. However, this option should not be used. Desired or necessary initialization settings should be set externally instead (i.e. through the mGuard). In case of a modem breakdown, the modem can then be replaced quickly without changing the modem settings.

☒ If the external modem is to be used for dial-ins, without the modem settings being entered accordingly, then you have to inform the modem that it should accept incoming calls after it rings. If you are using the extended HAYES instruction set, you add the character string `" AT&S0=1 OK"` (a space followed by `"AT&S0=1"`, followed by a space, followed by `"OK"`) to the initialization sequence.

☒ Some external modems, depending on their factory defaults, require a physical connection with the DTR cable of the serial port in order to operate correctly. Because the mGuard models do not provide this cable on the external serial port, you must add the character string `" AT&D0 OK"` (a space followed by `"AT&D0"`, followed by a space, followed by `"OK"`) to the above initialization sequence. In accordance with the extended HAYES instruction set, this sequence means that the modem does not use the DTR cable.

☒ If the external modem is to be used for dial-outs, it is connected to a private branch exchange, and if this private branch exchange does not generate a dial tone after the connection is opened, then the modem must be instructed not to wait for a dial tone before dialing. In this case, please add the character string `" ATX3 OK"` (a space followed by `"ATX3"`, followed by a space, followed by `"OK"`) to the initialization sequence. In this case, the control character `"W"` should be added to the "Phone number to call" on page 126, after the digit for an outside line, in order to wait for a dial tone.

### ➔ *mGuard industrial RS* with built-in modem / built-in ISDN modem (ISDN terminal adaptor)

The *mGuard industrial RS* can additionally have an optional built-in analog modem / built-in ISDN modem, also known as an ISDN terminal adaptor. If this is used, it must be configured. The built-in modem or built-in ISDN terminal adaptor can alternatively be used as follows:

- As a primary external interface, if the network mode is set to **Built-in Modem** under *Network ➔ Interfaces*, on the *General* tab page – see “Network ➔ Interfaces”, “General” on page 106. In this case, the data traffic is not made over the WAN port (= ethernet port) but over this modem.

OR

- As a secondary external interface, if the **secondary external interface** is activated and **Built-in Modem** is selected under *Network ➔ Interfaces*, on the *General* tab page – see “Network ➔ Interfaces”, “General” on page 106. In this case the data traffic is also made over the serial port.

OR

- For the PPP dialin option (see above under **Options for using the serial port**).

Note that the serial port of the device also provides similar usage options – see above. Thus, with the *mGuard industrial RS* with a built-in modem, for example, the normal data traffic can be made over a modem connection (*Modem* network mode) and simultaneously a second modem connection can be used for the PPP dialin option.

### For *mGuard industrial RS* with built-in modem

Additionally for *mGuard industrial RS* with built-in modem (analog)

External Modem	
Hardware handshake RTS/CTS	Off
Baudrate	57600
Handle modem transparently (for dial-in only)	Yes
Modem init string	"\d+++\dATH OK

Built-in Modem (analog)	
Country	Germany
Extension line (regarding dial tone)	No
Speaker volume (built-in speaker)	Low volume
Speaker control (built-in speaker)	Speaker is on during call establishment, but off when receiving carrier.

### External Modem

As for *mGuard industrial RS* (without a built-in modem), *mGuard blade*, *EAGLE mGuard*, and *mGuard delta*:

Configuration as above for **External Modem** – see above under “External Modem” on page 134.

### Built-in Modem (analog)

#### Country

The country where the *mGuard* and built-in modem is operated must be entered here. This ensures that the built-in modem works according to the valid remote access guidelines in the respective country and that it recognizes and uses dial tones correctly.

**Extension (outside line): Yes / No**

When **No** is selected, the mGuard waits for the dial tone when the telephone network is accessed and the mGuard calls the remote peer.

When **Yes** is selected, the mGuard does not wait for a dial tone. Instead, it begins dialing the remote peer immediately. This procedure is necessary when the installed mGuard modem is connected to a private extension that does not emit a dial tone when it is “picked up”. When a specific number must be dialed to access an external line (e.g. “0”), then this should be added to the beginning of the telephone number.

**Volume (built-in speaker)****Speaker use**

These settings define which sounds are emitted by the mGuard speakers and at which volume.

**For mGuard industrial RS with built-in ISDN terminal adaptor**

Additionally for  
mGuard industrial RS  
with built-in modem  
(ISDN)

**External Modem**

Hardware handshake RTS/CTS	Off
Baudrate	57600
Handle modem transparently (for dial-in only)	Yes
Modem init string	"\d+++dATH OK

**Built-in Modem (ISDN)**

1st MSN	
2nd MSN	
ISDN protocol	EuroISDN NET3
Layer-2 protocol	PPP/ML-PPP

**External Modem**

As for *mGuard industrial RS* (without a built-in modem), *mGuard blade*, *EAGLE mGuard*, and *mGuard delta*:

Configuration as above for **External Modem** – see above under “External Modem” on page 134

**Built-in Modem (ISDN)**

☒ These settings apply to the **Built-in Modem** network mode. In this network mode, data traffic is made over the built-in modem (installed ISDN terminal adaptor) and not over the mGuard WAN port.

**First MSN**

For outgoing calls, the mGuard transmits the entered MSN (Multiple Subscriber Number) to the called remote peer. The mGuard can also receive incoming calls over this MSN (provided dial-in is enabled – see **General** tab).

Max. 25 letters/numbers; the following special characters can be used: \*, #, : (colon)

**Second MSN**

If the mGuard can also receive incoming calls under another number, then enter the second MSN here.

### **ISDN protocol**

The EuroISDN (also known as NET3) ISDN protocol is used in Germany and many other European countries.

Otherwise the ISDN protocol is specified according to the country. If necessary, this must be requested from the relevant telephone company.

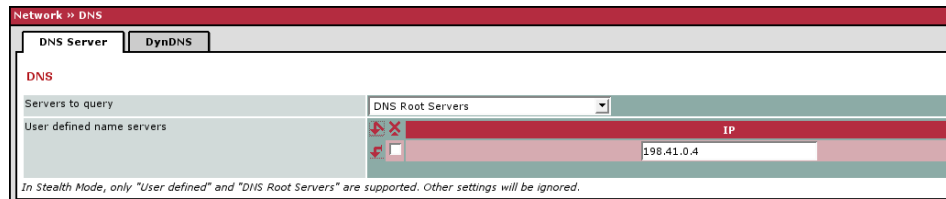
### **Layer 2 protocol**

This is the control equipment over which the local mGuard ISDN terminal adaptor communicates with the ISDN remote peer. This is generally the ISDN modem of the ISP used to create an Internet connection.

This must be requested from the ISP. PPP/ML-PPP is used very often.

## 6.4.2 Network → DNS

### DNS Server



When the mGuard has to initiate a connection on its own to a remote peer (e.g. a VPN gateway or a NTP server) and it is defined in hostname form (i.e. as in `www.example.com`) then the mGuard has to query a domain name server (DNS) for the IP address belonging to the host name.

If the mGuard is not in *Stealth* mode, locally connected clients can be configured to use the mGuard for releasing hostnames in IP addresses.

### DNS

#### Servers to query

Possible settings:

- DNS Root Servers
- Provider defined (e.g. via PPPoE or DHCP)
- User defined (servers listed below)

#### DNS Root Servers

Queries are sent to the root servers in the Internet whose IP addresses are stored in the mGuard. These addresses rarely change.

#### Provider defined (e.g. via PPPoE or DHCP)

The domain name server of the Internet Service Provider that provides access to the Internet is used. Only select this setting if the mGuard is operated in *PPPoE*, *PPTP*, *Modem* mode, or in *Router* mode with DHCP.

#### User defined (servers listed below)

If this setting is selected, the mGuard will connect to the domain name servers shown in the list of *User defined name servers*.

#### User defined name servers

You can enter the IP addresses of domain name servers in this list. If one of these should be used by the mGuard, select the option *User defined (servers listed below)* under **Servers to query**.

## DynDNS

At least one partner IP address must be known in order to establish a VPN connection so that they can connect to each other. This condition is not met if both participants are assigned IP addresses dynamically by their respective Internet Service Providers. In this case, a DynDNS service such as DynDNS.org or DNS4BIZ.com can be of assistance. The currently valid IP address is registered under a fixed name for a DynDNS service.

If you have registered with one of the DynDNS services supported by mGuard, you can enter the corresponding information in this dialog.

### Register this mGuard at a DynDNS Service? Yes / No

Select **Yes** if you have registered with a DynDNS provider and the mGuard should utilize this service. The mGuard reports its current IP address to the DynDNS service (i.e. the one assigned for Internet access by the Internet Service Provider).

### Refresh Interval (seconds)

Standard: 420 (seconds).

The mGuard informs the DynDNS service of its new IP address whenever the IP address of its Internet access is changed. For additional reliability, the device will also report its IP address at the interval set here.

This setting has no effect for some DynDNS providers like DynDNS.org as too many updates can cause the account to be closed.

### DynDNS Provider

The providers in this list support the same protocol as the mGuard.

Select the name of the provider where you are registered, e.g. DynDNS.org, TinyDynDNS, DNS4BIZ.

### DynDNS Server

Name of the server of the DynDNS provider selected above.

### DynDNS Login, DynDNS Password

Enter the user name and password assigned by the DynDNS provider here.

### DynDNS Hostname

The name selected for this mGuard at the DynDNS service, providing you use a DynDNS Service and have entered the corresponding data above.

Your computer (connected to the mGuard) is then accessible under this hostname.

### 6.4.3 Network → DHCP

The Dynamic Host Configuration Protocol (DHCP) can be used to automatically assign the appropriate network configuration to the clients connected to the mGuard. Under *Internal DHCP* you can configure the DHCP settings for the internal interface (LAN port) and under *External DHCP* the DHCP settings for the external interface (WAN port).

☒ The DHCP server is also operational in *Stealth* mode.

☒ IP configuration for Windows clients

When you start the mGuard DHCP server, you can configure the connected clients so that they obtain IP addresses automatically.

If you are using Windows XP, **Start, Control Panel, Network Connections**: Right-click on the LAN adaptor icon, then click on **Properties** in the pop-up menu. In the *LAN connection properties* local network on the *General* tab, select **Internet Protocol (TCP/IP)** under “This connection uses the following items” and then click on the **Properties** button.

Make the appropriate entries or settings in the *Internet Protocol Properties (TCP/IP)* dialog.

Internal/  
External DHCP



Mode

#### DHCP mode: Disabled / Server / Relay

Set this option to **Server** if the mGuard should function as an independent DHCP server. The selection settings are then displayed on the screen – see “DHCP mode → Server” on page 142.

Set the option to **Relay** if the mGuard should forward DHCP queries to another DHCP server. The selection settings are then displayed on the screen – see “DHCP mode → Relay” on page 144.

☒ The *Relay* DHCP mode is not supported in *Stealth* mode. If *Stealth* mode is in operation on the mGuard and *Relay* DHCP mode is selected, then this setting is ignored. However, DHCP client queries and the respective answers are forwarded due to the nature of *Stealth* mode.

If this option is set to **Disabled**, the mGuard does not answer any DHCP queries.

**DHCP mode → Server**

Network >> DHCP					
Internal DHCP External DHCP					
<b>Mode</b>					
DHCP mode	Server				
<b>DHCP Server Options</b>					
Enable dynamic IP address pool	Yes				
DHCP lease time	14400				
DHCP range start	192.168.1.100				
DHCP range end	192.168.1.199				
Local netmask	255.255.255.0				
Broadcast address	192.168.1.255				
Default gateway	192.168.1.1				
DNS server	10.0.0.254				
WINS server	192.168.1.2				
Static Mapping	<table border="1"> <thead> <tr> <th>Client MAC Address</th> <th>Client IP Address</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> </tbody> </table>	Client MAC Address	Client IP Address		
Client MAC Address	Client IP Address				

If the DHCP mode is set to *Server*, the following selection settings are displayed:

**DHCP Server Options****Enable dynamic IP address pool: Yes / No**

Select **Yes** if you wish to use the IP address pool defined by *DHCP range start* and *DHCP range end*.

Select **No** if you wish to use IP addresses statically assigned using the MAC address (see below).

**DHCP lease time**

Time in seconds for which the network configuration assigned to the client is valid. The client should renew its configuration shortly before this time expires. Otherwise it may be assigned to other computers.

**With enabled dynamic IP address pool:**

When the DHCP server and the dynamic IP address pool have been activated you can enter the network parameters to be used by the client:

**DHCP range start:** The start and end of the address range from

**DHCP range end:** which the mGuard's DHCP server should assign IP addresses to locally connected clients.

**Local netmask:** Defines the netmask of the client.  
The factory setting is: 255.255.255.0

**Broadcast address:** Defines the broadcast address of the client.

**Default gateway:** Defines which IP address should be used by the client as the default gateway. Usually this is the internal IP address of the mGuard.

<b>DNS server:</b>	Address of the server used by clients to resolve hostnames in IP addresses over the domain name service (DNS). If the DNS service of the mGuard is used, enter the internal IP address of the mGuard here.
<b>WINS server:</b>	Address of the server used by clients to resolve hostnames in addresses over the Windows Internet Naming Service (WINS).

### Static Mapping [according to MAC address]

Find out the MAC address of your client as follows:

**Windows 95/98/ME:** Start **winipcfg** in a DOS box.

**Windows NT/2000/XP:** Start **ipconfig /all** in a prompt. The MAC address is shown as “Physical Address”.

**Linux:** Call **/sbin/ifconfig** or **ip link show** in a shell.

You have the following options:

#### Client MAC address

The MAC address of the client (without spaces or hyphens).

#### Client IP address

The static IP of the client to be assigned to the MAC address.

- ☞ Static assignments take priority over the dynamic IP address pool.
- ☞ Static assignments and dynamic IP pool addresses must not overlap.
- ☞ Do not assign one IP address to several static MAC addresses, otherwise several MAC addresses are assigned to this IP address.
- ☞ Only use one DHCP server per subnetwork.

**DHCP mode → Relay**

Network >> DHCP

Internal DHCP External DHCP

**Mode**

DHCP mode Relay

**DHCP Relay Options**

DHCP Servers to relay to	IP
	192.168.89.45

Append Relay Agent Information (Option 82) No

If the DHCP mode is set to *Relay*, the following selection settings are displayed:

- ✘ The *Relay* DHCP mode is not supported in *Stealth* mode. If *Stealth* mode is in operation on the mGuard and *Relay* DHCP mode is selected, then this setting is ignored. However, DHCP client queries and the respective answers are forwarded due to the nature of *Stealth* mode.

**DHCP Relay Options****DHCP servers to relay to**

A list of one or more DHCP servers where DHCP requests are forwarded.

**Append Relay Agent Information (Option 82): Yes / No**

During forwarding, additional information according to RFC 3046 for the DNCP server can be added.

## 6.4.4 Network → Proxy Settings

### HTTP(S) Proxy Settings

Network >> Proxy Settings

HTTP(S) Proxy Settings

**HTTP(S) Proxy Settings**

Use Proxy for HTTP and HTTPS: No

HTTP(S) Proxy Server: proxy.example.com

Port: 3128

**Proxy Authentication**

Login:

Password:

A proxy server can be entered for the following mGuard administration connections:

- CRL download
- Firmware update
- Regular configuration profile retrieval from central peer
- Restoring licenses

### HTTP(S) Proxy Settings

#### Use Proxy for HTTP and HTTPS: Yes / No

When **Yes** is selected, connections using HTTP or HTTPS are transferred over a proxy server whose address and port is defined in the corresponding two fields.

#### HTTP(S) Proxy Server

Hostname or IP address of the proxy server.

#### Port

Port number to be used (e.g. 3128).

### Proxy Authentication

#### Login

User name for proxy server registration.

#### Password

Password for proxy server registration.

## 6.5 Authentication Menu

### 6.5.1 Authentication → Local Users

The term *local users* refers to users who have the right (depending on their authorization level), to configure the mGuard (*Root* and *Administrator* authorization levels) or to use it (*User* access permission).

#### Passwords

To login at a specific authorization level, the user must enter the corresponding password assigned to the level.

#### Authorization level

root	<p>Grants full rights to all parameters of the mGuard. Note: This is the only authorization level that allows you to setup an SSH connection to the device with which you can change the entire system settings beyond repair. Then only a flashing of the firmware can restore settings to the factory defaults (see “Flashing the firmware” on page 249).</p> <p>Default root password: <b>root</b></p>
administrator	<p>Grants all rights required for the configuration options accessed via the web-based administrator interface.</p> <p>Default user name: <b>admin</b> Default password: <b>mGuard</b></p> <p>The user name <b>admin</b> cannot be changed.</p>
user	<p>If a user password has been defined and activated, the user must enter this password to <u>enable an mGuard VPN connection</u> when they first attempt to access any HTTP URL. This must be made after every restart of the mGuard. To use this option, enter the desired user password once in each of the corresponding entry fields.</p>

**root****Root Password (Account: root)**

Default setting: **root**

To change the root password, enter the current password in the *Old Password* field, then the new password in the two corresponding fields directly underneath.

**admin****Administrator Password (Account: admin)**

Default setting: **mGuard**

(fixed user name: admin)

**user****Disable VPN until the user is authenticated via HTTP: Yes / No**

The factory default for this option is **No**.

If **Yes** is selected, VPN connections can only be used after a user has logged into the mGuard via HTTP.

As long as authentication is required, all HTTP traffic is redirected to the mGuard.

Changes to this option become active after the next reboot.

**User Password**

There is no factory default for the user password. To set one, enter the desired password twice – once in each of the two entry fields.

## 6.5.2 Authentication → Firewall Users

For example to eliminate private surfing on the Internet, every outgoing connection is blocked by the *outgoing filter rules* listed under *Network Security → Packet Filters*. VPN is not affected by this. Under *Network Security → User Firewall*, certain users can be assigned different firewall definitions (e.g. outgoing connections are permitted). This user firewall rule comes into effect as soon as the respective firewall user has logged in (see “Network Security → User Firewall” on page 178).

### Firewall Users

Authentication → Firewall Users			
Firewall Users	RADIUS Servers	Access	Status
<b>Users</b>			
Enable user firewall	No		
Enable group authentication	No		
User Name	Authentication Method	User Password	
Bob	RADIUS		

### Users

Lists the firewall users by their user names. Also defines the authentication methods.

#### Enable user firewall: Yes / No

Under the *Network Security → User Firewall* menu, firewall rules can be defined and assigned to specific firewall users.

By selecting **Yes**, the firewall rules for the listed users are activated as soon as the corresponding user logs in.

#### Enable group authentication: Yes / No

If enabled, the mGuard forwards login requests for unknown users to the RADIUS server. If successful, the reply from the RADIUS server will contain a group name. The mGuard then enables user firewall templates containing this group name as the template user.

The RADIUS server must be configured to deliver this group name in the “Access Accept” package as a “Filter-ID=<groupname>” attribute.

#### Username

Required name of the user during login.

#### Authentication Method: RADIUS / Local DB

##### Local DB:

When *Local DB* is selected, the password assigned to the user must be entered in the *User Password* column, next to the *User Name*.

##### RADIUS:

When RADIUS is selected, the user password can be stored on the RADIUS server.

#### User Password

Only active when Local is selected as authentication method.

## RADIUS Servers

The screenshot shows the 'Authentication > Firewall Users' menu with tabs for 'Firewall Users', 'RADIUS Servers', 'Access', and 'Status'. The 'RADIUS Servers' tab is active. It displays fields for 'RADIUS timeout' (set to 3) and 'RADIUS retries' (set to 3). Below these is a table with columns 'Server', 'Port', and 'Secret'. One server is listed: 'radius.company.local' on port '1812' with secret 'cah5lt4et0sa7eepha'.

### RADIUS Servers

#### RADIUS timeout

Specifies (in seconds) how long the mGuard waits for an answer from the RADIUS server. Standard: 3 seconds

#### RADIUS retries

Specifies how often requests to the RADIUS server are retried after a RADIUS timeout has occurred. Standard: 3

#### Server

Name of the RADIUS server or its IP address

#### Port

The port number used by the RADIUS server

#### Secret

RADIUS server password

## Access

The screenshot shows the 'Authentication > Firewall Users' menu with tabs for 'Firewall Users', 'RADIUS Servers', 'Access', and 'Status'. The 'Access' tab is active. It displays the 'HTTPS Authentication via' section with an 'Interface' dropdown menu set to 'External'. A note at the bottom states: 'Please note: Login of firewall users is possible only via the interfaces listed above if HTTPS remote access is enabled therefor as well (see Management > Web Settings)'.

### HTTPS Authentication via

#### Interface: External / Internal / External 2 / Dial-in<sup>1</sup>

Specifies which mGuard interfaces firewall users can use to log into the mGuard. For the interface selected, web access via HTTPS must be enabled:

**Management** menu, **Web Settings**, **Access** tab page. See “Access” on page 73.

## Status

The screenshot shows the 'Authentication > Firewall Users' menu with tabs for 'Firewall Users', 'RADIUS Servers', 'Access', and 'Status'. The 'Status' tab is active. It displays the 'Status' section with the message: 'The User Firewall is not enabled.'

If the user firewall is activated, its status is displayed here.

1. *External 2* and *Dial-in* only for devices with serial ports.  
See “Network → Interfaces” on page 105.

### 6.5.3 Authentication → Certificates

#### Definition



Authentication is a fundamental element of secure communication. The X.509 authentication procedure ensures that the “correct” partners communicate with each other. Certificates are used in this process. An “incorrect” communication partner is one who falsely identifies themselves as someone they are not, see glossary under “X.509 certificate”.

#### Certificate

A certificate is used as proof of authentication for its owner. The relevant authorizing party in this case is the CA (Certificate Authority). The digital signature on the certificate is made by the CA. By providing this signature, the CA confirms that the authorized certificate owner possesses a private key that corresponds to the public key in the certificate.

The name of the certificate provider is shown as *Issuer* on the certificate, whilst the name of the certificate owner is shown as *Subject*.

#### Self-signed certificates

A self-signed certificate is one that is signed by the certificate owner, and not by a CA. In self-signed certificates, the name of the certificate owner is shown as both *Issuer* and *Subject*.

Self-signed certificates are used when communication partners want to use the X.509 authentication procedure without having an official certificate. This type of authentication should only be used between partners that know and trust each other well. Otherwise, from a security point of view such certificates are as worthless as a self-made passport without the official stamp.

Certificates are shown to all communication partners (users or machines) during the connection process, providing the X.509 authentication method is used.

In terms of mGuard, this could relate to the following applications:

- Authentication of communication partners during establishment of VPN connections – see “IPsec VPN → Connections”, “Authentication” on page 207
- mGuard management using SSH (shell access) – see “Management → System Settings”, “Shell Access” on page 65
- mGuard management using HTTPS – see “Management → Web Settings”, “Access” on page 73

#### Certificate, machine certificate

Certificates can be used to identify (authenticate) oneself to others.

The certificate used by the mGuard to identify itself to others shall be known as the “machine certificate” here, in line with Microsoft Windows terminology.

A “certificate”, “certificate specific to an individual” or “user certificate displaying a person” is one used by operators to authenticate themselves to remote peers (e.g. for an operator attempting remote access to the mGuard using HTTPS and a web browser). When acquired by a web browser, a certificate specific to an individual can be saved on a chip card and then inserted into the card reader of the owner's computer.

**Remote certificate**

A certificate is thus used by its owner (person or machine) as a form of ID in order to verify that they really are the individual they identify themselves as. As there are two communication partners, the process takes place alternately: Partner A shows their certificate to their remote peer (partner B). Partner B then shows their certificate to their remote peer (partner A).

In order for A to accept the certificate shown by B (thus allowing communication), there is the following option: A has earlier received a copy of the certificate from B (e.g. by data carrier or email), with which B will verify itself. A can then verify the certificate shown later by B by comparing it to this certificate. When related to the mGuard interface, the certificate copy given here by B to A is an example of a *Remote certificate*.

For bilateral authentication to take place, both partners must thus give each other a copy of their certificate. A installs the copy of the certificate from B as its remote certificate. B then installs the copy of the certificate from A as its remote certificate.

⊗ Never give the PKCS#12 file (file name extension: \*.p12) as a copy to the remote peer in order to use X.509 authentication at a later time! The PKCS#12 file contains a private key that must be kept secret and must not be given to a third party. See “Creation of certificates” on page 152.

To create a copy of a machine certificate imported in the mGuard, proceed as follows:

Click the **Current certificate file** button on the machine certificate tab next to the row title *Download certificate* (see “Machine Certificates” on page 156).

**CA certificates**

The certificate shown by a remote peer can also be checked by the mGuard in a different way (i.e. not by consulting the locally installed remote certificate on the mGuard). To check the authentication of remote peers using X.509, the method of consulting CA certificates can be used instead or as a supplement.

CA certificates provide a way of checking whether the certificate shown by the remote peer is really signed by the CA entered within.

A CA certificate is available from the related CA (file name extension: \*.cer, \*.pem or \*.crt). It is often available to download from the website of the CA itself.

The mGuard can then check if the certificate shown by the remote peer is authentic using CA certificates. In this case, all CA certificates must be available in mGuard in order to build a chain with the certificate displayed by the remote peer. Aside from the CA certificate, whose signature can be seen in the displayed certificate of the remote peer to be checked, the CA certificate of the superordinate CA up to the root certificate must be used (see glossary under CA certificate).

Authentication using CA certificates allows an expansion in the number of possible remote peers without any increased management output, as the installation of a remote certificate for each possible remote peer is not compulsory.

## Creation of certificates

For certificate creation, a *private key* and the corresponding *public key* are needed. Programs are provided where any user can create these keys. A certificate with the relevant *public key* can also be created, resulting in a self-signed certificate. Further documentation on self-creation can be downloaded from [www.innominat.de](http://www.innominat.de). This can be found in the download area as an application note under the title “How to obtain X.509 certificates”.

A related certificate signed by a CA must be requested from the CA.

In order for the private key to be imported to the mGuard with the related certificate, these components must be packed into a PKCS#12 file (file name extension: \*.p12).

## Authentication procedure

The mGuard can use two principle procedures for X.509 authentication.

- The authentication of a remote peer is carried out on the basis of the certificate ⇔ remote certificate. In this case, the consulted remote certificate must be given for each individual connection (e.g. for VPN connections).



AND / OR

- The mGuard consults the provided CA certificate to check whether the certificate shown by the remote peer is authentic. In this case, all CA certificates must be available in mGuard in order to build a chain up to the root certificate using the certificate displayed by the remote peer.



“Available” means that the corresponding CA certificates must be installed in the mGuard (see “CA Certificates” on page 158) and must be made available additionally during the configuration of the corresponding applications (SSH, HTTPS, VPN).

Whether both procedures are used alternatively or in combination varies on the application (VPN, SSH and HTTPS). Consult the following tables for more details.

**SSH: Authentication for SSH**

<b>The remote peer shows the following:</b>	Certificate (specific to individual) <b>signed by CA</b>	Certificate (specific to individual) <b>self-signed</b>
<b>The mGuard authenticates the remote peer using:</b>		
	<p>All CA certificates that build the chain to the root CA certificate together with the certificates displayed by the remote peer</p> <p>or ADDITIONALLY</p> <p>Remote certificates, <u>if</u> used as filter (See "6.2.1 Management → System Settings", "Shell Access" on page 65)</p>	Remote Certificate

**HTTPS: Authentication for HTTPS**

<b>The remote peer shows the following:</b>	Certificate (specific to individual) <b>signed by CA*</b>	Certificate (specific to individual) <b>self-signed</b>
<b>The mGuard authenticates the remote peer using:</b>		
	<p>All CA certificates that build the chain to the root CA certificate together with the certificates displayed by the remote peer</p> <p>or ADDITIONALLY</p> <p>Remote certificates, <u>if</u> used as filter (See "6.2.2 Management → Web Settings", "Access" on page 73)</p>	Remote Certificate

\* The remote peer can additionally provide sub-CA certificates. In this case the mGuard can form the set union for building the chain from the provided CA certificates and the self-configured CA certificates. The corresponding root CA certificate of the mGuard must always be available.

**VPN: Authentication for VPN**

The remote peer shows the following:	Machine certificate signed by CA	Machine certificate self-signed
The mGuard authenticates the remote peer using:	↕	↕
	Remote Certificate  OR  All CA certificates that build the chain to the root CA certificate together with the certificates displayed by the remote peer	Remote Certificate

**Important:** Installation of the certificate in the mGuard under *Authentication* → *Certificates* is not sufficient. In addition, which mGuard certificate imported from the pool is used must be referenced in the relevant applications (VPN, SSH, HTTPS).

☒ The remote certificate for authentication of a VPN connection (or VPN connection channels) is installed in the *IPsec VPN* → *Connections* menu.

**Certificate settings**

**Authentication > Certificates**

**Certificate settings**

Check the validity period of certificates and CRLs: No

Enable CRL checking: No

CRL download interval: Never

**Certificate settings**

The settings made here relate to all certificates and certificate chains checked by the mGuard.

The following are excepted:

- Self-signed certificates from remote peers
- VPN of all remote certificates

**Check the validity period of certificates and CRLs: No / Wait for system time synchronization**

**No:** The entered validity periods in certificates and CRLs are ignored by the mGuard.

**Wait for system time synchronization**

The validity periods entered in certificates and CRLs are only considered by the mGuard when the current date and time are known:

- Through the installed clock (for *mGuard industrial RS* and *mGuard delta*)
- By synchronizing the system time. See “Time and Date” on page 62.

Up until this point, all certificates are considered as invalid.

**Enable CRL checking: Yes / No**

**Yes:** When CRL checking is enabled, the mGuard consults the CRL (Certificate Revocation List) and checks whether the mGuard certificates are blocked or not.

CRLs are issued by the CA and contain the serial numbers of blocked certificates (e.g. certificates have been manipulated or stolen).

Enter the origin of the CRL under the **CRL** tab (see “CRL” on page 161).

- ☒ When CRL checking is enabled, a CRL must be configured for each *Issuer* of certificates in the mGuard. Absent CRLs lead to certificates being declared invalid.
- ☒ CRLs are verified by the mGuard using a relevant CA certificate. Therefore, all CA certificates belonging to a CRL (i.e. all sub-CA certificates and the root certificate) must be installed on the mGuard. If the validity of a CRL cannot be proven, then it is ignored by the mGuard.
- ☒ If the use of CRLs is activated together with the consideration of validity periods, lists are ignored if their validity period has expired or has not yet started.

**CRL download interval**

If *Enable CRL checking* is set to **Yes** (see above), then select here the time period after which the CRLs should be downloaded and applied.

Enter the origin of the CRL under the **CRL** tab (see “CRL” on page 161).

If CRL checking is activated but the CRL download is set to **Never**, then the CRL must be manually loaded on the mGuard so that CRL checking can be made.

## Machine Certificates

The mGuard authenticates itself to the remote peer using a machine certificate in the local mGuard. The machine certificate is the “passport” of an mGuard with which it can authenticate itself to the respective remote peer.

For more details, see “Authentication → Certificates” on page 150.

By importing a PKCS#12 file, the mGuard obtains a private key and the corresponding machine certificate. Several PKCS#12 files can be loaded into the mGuard. The mGuard can then show the remote peer a self-signed certificate or certificate signed by the CA for different connections.

☒ In order to use the installed machine certificate, it must be referenced additionally during the configuration of applications (SSH, VPN) so that it can be used for the respective connection or remote access type.

Example of imported machine certificates:

The screenshot displays the 'Machine Certificates' tab in the mGuard configuration interface. It lists three certificates with the following details:

Subject	Subject Alternative Names	Issuer	Validity	Fingerprint	Shortname	Upload PKCS#12	Download Certificate
CN=mguard.m.customer.co.uk,L=M,O=Sample Customer,C=UK		CN=Web-SubCA 01,O=Sample Web Securities Inc.,C=UK	From Jun 20 11:27:05 2007 GMT to Jun 20 11:27:05 2010 GMT	MDS: 17:57:2F:50:FF:44:5E:8D:D2:E3:A2:CF:91:B5:1B:A8 SHA1: 66:E5:C8:EE:A9:EC:D0:C3:19:0C:7C:0B:75:C8:B7:7D:62:79:0B:B9	mguard.m.customer.co.uk	Filename: <input type="text"/> Browse... Import Password: <input type="password"/>	Current Certificate File
CN=mguard.l.customer.co.uk,L=L,O=Sample Customer,C=UK		CN=SSH-SubCA 01,O=Secure Access Ltd.,C=UK	From Jun 20 12:08:17 2007 GMT to Jun 20 12:08:17 2010 GMT	MDS: E8:61:C3:B3:8F:03:E1:5A:91:4E:C2:96:64:B0:4B:DD SHA1: B0:A2:02:35:4E:10:BE:A4:F2:11:BB:A9:D8:F1:EB:C4:12:88:7B:21	mguard.l.customer.co.uk	Filename: <input type="text"/> Browse... Import Password: <input type="password"/>	Current Certificate File
CN=VPN terminal machine 01,L=S,O=Sample Supplier,C=UK		CN=VPN-SubCA 01,O=Sample Supplier,C=UK	From Jun 20 12:05:03 2007 GMT to Jun 20 12:05:03 2010 GMT	MDS: C6:A6:A7:0B:0B:5C:4F:A0:BB:67:C2:F6:2A:5B:E6:74 SHA1: AD:CC:20:4B:B5:FD:8D:DE:29:A1:71:4B:8B:6B:4E:C5:B6:F6:CA	VPN terminal machine 01	Filename: <input type="text"/> Browse... Import	

### Machine Certificates

Shows the currently imported X.509 certificates that the mGuard uses to authenticate itself to remote peers (e.g. other VPN gateways).

To import a new certificate, please proceed as follows:

### Importing a new machine certificate

#### Requirement:

The PKCS#12 file (format: \*.p12 or \*.pfx) is saved on the connected computer.

Proceed as follows:

1. Click on **Browse...** to select the file.
2. Enter the password that is used for protection of the PKCS#12 file private key in the *Password* field.
3. Click on **Import**.

After the import, the installed certificate can be seen under *Certificate*.

**Shortname**

During the machine certificate import process, the CN attribute from the certificate subject field is suggested as the short name (providing the *Shortname* field is empty at this point). This name can be adopted or another name can be chosen.

Name entry (whether the suggested one or another) is mandatory. The names must be unique and must not be used more than once.

**Use of the short name:** During the configuration of

- SSH (Menu *Management* → *System settings, Shell access*),
- HTTPS (Menu *Management* → *Web settings, Access*) and
- VPN connections (Menu *IPsec VPN* → *Connections*)

the imported certificates in the mGuard are given as a selection list. The certificates are displayed under the short name entered for each individual certificate. For this reason, the entry of a name is necessary.

**Creating a certificate copy**

You can make a copy of the imported machine certificate (e.g. for the remote peer so that this mGuard can authenticate itself). This copy does not contain the private key, and can be made public at any time.

To do this, proceed as follows:

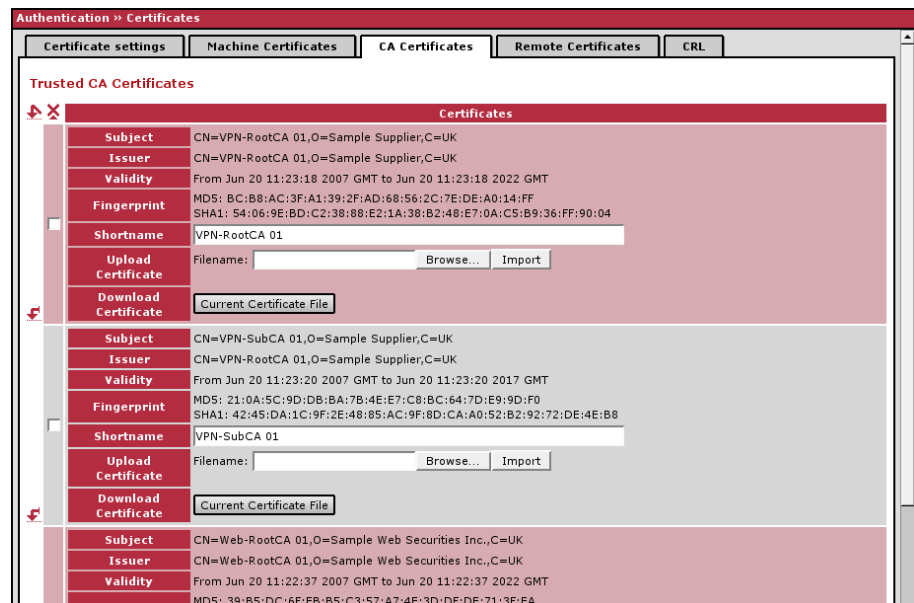
Click on the **Current Certificate File** button on the machine certificate next to the *Download certificate* row title. Make the desired entries in the dialog that opens.

## CA Certificates

CA certificates are those from a Certificate Authority (CA). CA certificates are used to check whether the certificates shown by remote peers are authentic.

The check is made as follows: The issuing authority (CA) is entered as Issuer in the certificate shown by the remote peer. These details can be checked for authenticity by the same Issuer using the local CA certificate. For more details, see “Authentication → Certificates” on page 150.

Example of imported CA certificates:



### Trusted CA Certificates

Shows the current imported CA certificates.

To import a new certificate, please proceed as follows:

### Importing a new CA certificate

#### Requirement:

The file (file name extension: \*.cer, \*.pem or \*.crt) is saved on the connected computer.

Proceed as follows:

1. Click on **Browse...** to select the file.
2. Click on **Import**.

After the import, the installed certificate can be seen under *Certificate*.

### Shortname

During the CA certificate import process, the CN attribute from the certificate subject field is suggested as the short name (providing the “shortname” field is empty at this point). This name can be adopted or another name can be chosen.

Name entry (whether the suggested one or another) is mandatory. The names must be unique and must not be used more than once.

**Use of the short name:** During the configuration of

- SSH (Menu *Management* → *System settings, Shell access*),
- HTTPS (Menu *Management* → *Web settings, Access*) and
- VPN connections (Menu *IPsec VPN* → *Connections*)

the imported certificates in the mGuard are given as a selection list.

The certificates are displayed under the short name entered for each individual certificate. For this reason, the entry of a name is necessary.

## Creating a certificate copy

You can make a copy of the imported CA certificate.

To do this, proceed as follows:

Click on the **Current Certificate File** button on the CA certificate next to the *Download certificate* row title. Make the desired entries in the dialog that opens.

## Remote certificates

A remote certificate is a copy of the certificate that is used by a remote peer to authenticate itself to the mGuard. Remote certificates are files received through a trustworthy channel from operators of possible remote peers (file name extension: \*.cer, \*.pem or \*.crt). Load these files onto the mGuard so that bilateral authentication can take place. The remote certificates of several possible remote peers can be installed.

☒ The remote certificate for authentication of a VPN connection (or VPN connection channels) is installed in the *IPsec VPN → Connections* menu.

For more details, see “Authentication → Certificates” on page 150.

Example of imported remote certificates:

The screenshot shows the 'Authentication > Certificates' window with the 'Remote Certificates' tab selected. It displays a list of 'Trusted remote Certificates' with the following details:

Subject	Issuer	Validity	Fingerprint	Shortname	Upload Certificate	Download Certificate
CN=Meyer\, Ralf,L=B,OU=Service,O=Sample Supplier,C=UK	CN=Web-SubCA 01,O=Sample Web Securities Inc.,C=UK	From Jun 20 11:27:08 2007 GMT to Jun 20 11:27:08 2010 GMT	MD5: 1D:EF:40:76:D1:52:F8:07:18:0B:6D:F7:85:93:37:6D SHA1: C8:DC:97:2E:B7:1D:6A:94:EE:FE:6D:6B:71:58:F1:35:52:D3:BE:E1	Meyer, Ralf	Filename: <input type="text"/> Browse... Import	Current Certificate File
CN=Wirth\, Nicola,L=B,OU=Service,O=Sample Supplier,C=UK	CN=Web-SubCA 01,O=Sample Web Securities Inc.,C=UK	From Jun 20 11:27:11 2007 GMT to Jun 20 11:27:11 2010 GMT	MD5: 09:98:7B:71:58:F5:F6:CF:EA:28:BF:95:6C:8E:A3:7F SHA1: E3:C3:0F:2E:EC:3D:94:9C:A9:E5:BD:7B:E0:B9:F9:36:E6:D3:0C:9A	Wirth, Nicola	Filename: <input type="text"/> Browse... Import	Current Certificate File
CN=Schlau\, Heiner,L=B,OU=Service,O=Sample Supplier,C=UK	CN=Web-SubCA 01,O=Sample Web Securities Inc.,C=UK	From Jun 20 11:27:13 2007 GMT to Jun 20 11:27:13 2010 GMT	MD5: E1:A3:14:0B:09:87:93:AA:AC:42:4C:38:3D:1D:BD:79 SHA1: 15:C2:75:EF:12:6E:8A:23:2D:4C:72:72:8B:1A:DF:99:EB:61:89:A2	Schlau, Heiner	Filename: <input type="text"/> Browse... Import	Current Certificate File
CN=Findig\, Petra,L=B,OU=Service,O=Sample Supplier,C=UK	CN=Web-SubCA 01,O=Sample Web Securities Inc.,C=UK	From Jun 20 11:27:15 2007 GMT to Jun 20 11:27:15 2010 GMT	MD5: 83:80:FA:A1:7E:A2:C0:77:FB:39:D1:06:7E:12:E3:91			

### Trusted remote Certificates

Shows the current imported remote certificates.

To import a new certificate, please proceed as follows:

### Importing a new certificate

#### Requirement:

The file (file name extension: \*.cer, \*.pem or \*.crt) is saved on the connected computer.

Proceed as follows:

1. Click on **Browse...** to select the file.
2. Click on **Import**.

After the import, the installed certificate can be seen under *Certificate*.

### Shortname

During the remote certificate import process, the CN attribute from the certificate subject field is suggested as the short name (providing the *Shortname* field is empty at this point). This name can be adopted or another name can be chosen.

Name entry (whether the suggested one or another) is mandatory.  
The names must be unique and must not be used more than once.

**Use of the short name:** During the configuration of

- SSH (Menu *Management* → *System settings, Shell access*) and
- HTTPS (Menu *Management* → *Web settings, Access*)

the imported certificates in the mGuard are given as a selection list.

The certificates are displayed under the short name entered for each individual certificate. For this reason, the entry of a name is necessary.

### Creating a certificate copy

You can make a copy of the imported remote certificate.

To do this, proceed as follows:

Click on the **Current Certificate File** button on the remote certificate next to the *Download certificate* row title. Make the desired entries in the dialog that opens.

## CRL

The screenshot shows the 'Authentication » Certificates' section with the 'CRL' tab selected. The interface includes a table with the following headers: Issuer, Last Update, Next Update, URL, and Upload. Below the table, there are 'Browse...' and 'Import' buttons. The table is currently empty.

## CRL

CRL = Certificate Revocation List

The CRL is a list containing the serial numbers of blocked (revoked) certificates.

This page is used for the configuration of sites where the mGuard should download CRLs in order to use them.

☒ Certificates are only checked when **Yes** is set under **Enable CRL checking**.  
See “Certificate settings” on page 154.

☒ A CRL with the same issuer name must be present for each issuer name entered in the checked certificate. If a CRL is absent and CRL checking is enabled, then the certificate is declared invalid.

**Issuer**

Only displays information that the mGuard reads directly from the CRL:

Shows the issuer of the affected CRL.

**Last Update**

Only displays information that the mGuard reads directly from the CRL:

Time and date of creation for CRL currently present on the mGuard.

**Next Update**

Only displays information that the mGuard reads directly from the CRL:

Estimated time and date when the CA will next issue a new CRL.

☒ These entries are not influenced by the CRL download interval.

**URL**

Enter the CA URL where CRL downloads are obtained from if the CRL is downloaded on a regular basis (as defined in the **CRL download interval** under the *Certificate settings* tab (see “Certificate settings” on page 154)).

**Upload**

If the CRL is present in file form, then it can be loaded onto the mGuard manually.

To do this, click on the **Browse...** button, then select the file and click on **Import**.

## 6.6 Network Security Menu (not for blade controller)

### 6.6.1 Network Security → Packet Filter

The mGuard comes with an integrated *Stateful Packet Inspection Firewall*. The connection data for each active connection is collected in a database (connection tracking). Therefore, it is only necessary to define rules for one direction. Only data from the opposite direction of the connection is allowed through, and none other. A side-effect is that existing connections are not cancelled during reconfiguration, even if a corresponding new connection can no longer be setup.

#### Factory defaults for the firewall:

- All incoming connections are rejected (except VPN).
- Data packets of all outgoing connections are passed through.

Firewall rules have an effect on the firewall that is constantly active, with the exception of:

- **VPN connections.** Individual firewall rules are defined for VPN connections – see “IPsec VPN → Connections”, “Firewall” on page 213.
- **User firewall.** If a user logs in with defined firewall rules, then these take priority (see “Network Security → User Firewall” on page 178). After this, the constantly active firewall rules then come into effect.

☒ The anti-virus function (see “Web Security → HTTP” on page 182, “Web Security → FTP” on page 185, “Email Security → POP3” on page 188, “Email Security → SMTP” on page 191) has priority over the firewall rules defined here and can partially override them. This behavior can be overridden in the **Network Security → Packet Filters, Advanced** menu by setting the option to **Connections scanned for viruses are subject to firewall rules** – see “Advanced”, “AntiVirus Scanning” on page 170.

☒ If multiple firewall rules are set, they will be searched in the order in which they are listed (top-down) until a suitable rule is found. This rule is then applied. If there are other suitable rules further down the list, then these are ignored.

### Incoming Rules

The screenshot shows the 'Incoming Rules' tab in the 'Network Security >> Packet Filter' configuration window. It features a table with columns: N#, Interface, Protocol, From IP, From Port, To IP, To Port, Action, Comment, and Log. A single rule is listed with N# 1, Interface 'External', Protocol 'TCP', From IP '0.0.0.0/0', From Port 'any', To IP '0.0.0.0/0', To Port 'any', Action 'Accept', and Log 'No'. Below the table, there is a note: 'These rules specify which traffic from the outside is allowed to pass to the inside. Please note: Port settings are only meaningful for TCP and UDP!'. At the bottom, there is a checkbox for 'Log entries for unknown connection attempts?' which is currently set to 'No'.

N#	Interface	Protocol	From IP	From Port	To IP	To Port	Action	Comment	Log
1	External	TCP	0.0.0.0/0	any	0.0.0.0/0	any	Accept		No

These rules specify which traffic from the outside is allowed to pass to the inside.  
Please note: Port settings are only meaningful for TCP and UDP!

Log entries for unknown connection attempts? ☐ No

#### Incoming

Lists the firewall rules that have been set. These rules apply for incoming data connections that were initiated externally.

If no rule has been set, the data packets for all incoming connections (except VPN) are dropped (factory default).

You have the following options:

**Interface: External / External 2 / Any External<sup>1</sup>**

Specifies over which interface the data packets come in so that the rule applies to them. **Any External** refers to the **External** and **External 2** interfaces. These interfaces are only available for mGuard models that have a serial port with external access.

**Protocol**

TCP, UDP, ICMP, All.

**From IP / To IP**

**0.0.0.0/0** means all IP addresses. To enter an address, use CIDR notation – see “CIDR (Classless Inter-Domain Routing)” on page 246.

**From Port / To Port**

(Only evaluated for TCP and UDP protocols)

**any** describes any selected port.

**startport:endport** (e.g. 110:120) defines a range of ports.

You can specify individual ports by giving either their port number or the corresponding service name: (e.g. 110 for pop3 or pop3 for 110).

**Action**

**Accept** means that data packets may pass through.

**Reject** means that the data packets are rejected. The sender is informed that the data packets have been rejected. In *Stealth* mode, Reject has the same effect as Drop – see below.

**Drop** means that data packets may not pass through. The data packets are discarded and the sender is not informed of their whereabouts.

**Name** of set of rules, if defined. When the name of a set of rules is entered, the firewall rules saved under this name come into effect – see the *Sets of Rules* tab.

☒ In Stealth mode, **Reject** has the same effect as **Drop**.

**Comment**

Freely selectable comment for this rule.

**Log**

For each individual firewall rule you can specify whether the use of the rule

- should be logged (set *Log* to **Yes**) or
- should not be logged (set *Log* to **No** – factory default)

**Log entries for unknown connection attempts?: Yes / No**

When set to **Yes**, all attempts to establish a connection that are not covered by the rules defined above are logged (factory default: **No**).

---

1. *External 2* and *Any External* only for devices with serial ports.  
See “Network → Interfaces” on page 105.

## Outgoing Rules

Network Security » Packet Filter

Incoming Rules Outgoing Rules Sets of Rules MAC Filtering Advanced

Outgoing

Log ID: fw-outgoing-N<sup>o</sup>-3e8b12d5-3d40-1fd9-97e6-

N <sup>o</sup>	Protocol	From IP	From Port	To IP	To Port	Action	Comment
1	All	0.0.0.0/0	any	0.0.0.0/0	any	Accept	default rule

These rules specify which traffic from the inside is allowed to pass to the outside.  
Please note: Port settings are only meaningful for TCP and UDP!

Log entries for unknown connection attempts? No

### Outgoing

Lists the firewall rules that have been set. These rules apply for outgoing data connections that were initiated internally in order to communicate with a remote peer.

**Factory default:** A rule is set that allows all outgoing connections.

If no rule is set, then all outgoing connections are forbidden (except VPN).

☒ The anti-virus function (see “Web Security → HTTP” on page 182, “Web Security → FTP” on page 185, “Email Security → POP3” on page 188, “Email Security → SMTP” on page 191) has priority over the firewall rules defined here and can partially override them. This behavior can be overridden in the **Network Security → Packet Filters, Advanced** menu by setting the option to **Connections scanned for viruses are subject to firewall rules** – see “Advanced”, “AntiVirus Scanning” on page 170.

You have the following options:

#### Protocol

TCP, UDP, ICMP, All.

#### From IP / To IP

**0.0.0.0/0** means all IP addresses. To enter an address, use CIDR notation – see “CIDR (Classless Inter-Domain Routing)” on page 246.

#### From Port / To Port

(Only evaluated for TCP and UDP protocols)

**any** describes any selected port.

**startport:endport** (e.g. 110:120) defines a range of ports.

You can specify individual ports by giving either their port number or the corresponding service name: (e.g. 110 for pop3 or pop3 for 110).

#### Action

**Accept** means that data packets may pass through.

**Reject** means that the data packets are rejected. The sender is informed that the data packets have been rejected. In *Stealth* mode, Reject has the same effect as Drop – see below.

**Drop** means that data packets may not pass through. The data packets are discarded and the sender is not informed of their whereabouts.

**Name** of set of rules, if defined. When the name of a set of rules is entered, the firewall rules saved under this name come into effect – see the *Sets of Rules* tab.

☒ In Stealth mode, **Reject** has the same effect as **Drop**.

**Comment**

Freely selectable comment for this rule.

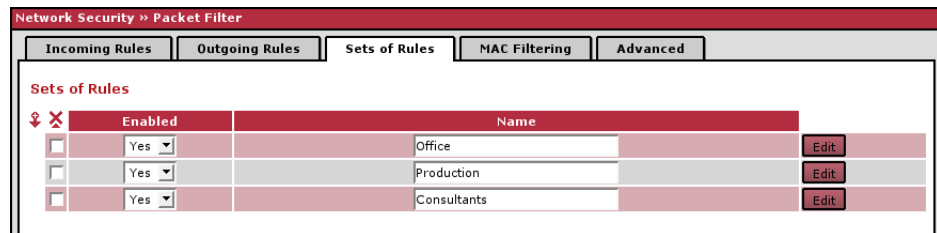
**Log**

For each individual firewall rule you can specify whether the use of the rule

- should be logged (set *Log* to **Yes**) or
- should not be logged (set *Log* to **No** – factory default)

**Log entries for unknown connection attempts?: Yes / No**

When set to **Yes**, all attempts to establish a connection that are not covered by the rules defined above are logged (factory default: **No**).

**Sets of Rules**

Sets of rules are defined and stored for structuring incoming and outgoing rules. A set of rules can then be referred to in an incoming or outgoing rule, so that the rules contained within the set of rules are applied there.

It is also possible to refer to another defined set of rules when defining a set of rules (i.e. inserting this as a module in the current set of rules).

**Sets of Rules**

Lists all defined sets of firewall rules.

**Making a new set of rules definition:**

Click on the **Edit** button on the right side of the set of rules table under the “(unnamed)” entry.

If the “(unnamed)” entry cannot be seen, then open a further line in the set of rules table.

**Editing a set of rules:**

Click on the **Edit** button to the right of the entry.

- ☒ If a set of firewall rules is comprised of multiple firewall rules, they are searched in the order in which they are listed (top-down) until a suitable rule is found. This rule is then applied. If there are other suitable rules further down the list, then these are ignored.

**Enabled: Yes / No**

Activates / deactivates the relevant set of rules.

**Name**

Name of the set of rules. The name is defined during creation of the set of rules.

The *Set of Rules* page is displayed after clicking on the **Edit** button:

Network Security > Packet Filter > Office Protocols

**Set of Rules**

**General**

A descriptive name for the set: Office Protocols

Enabled: Yes

**Firewall rules**

Log ID: fw-ruleset-000-W0-3e8b12d7-3640-1f69-97e6-000d0e0220d7

No	Protocol	From IP	From Port	To IP	To Port	Action	Comment	Log
1	TCP	0.0.0.0/0	any	10.1.66.7	smtp	Accept		No
2	TCP	0.0.0.0/0	any	10.1.66.8	pop3	Accept		No
3	TCP	0.0.0.0/0	any	10.1.66.8	imap	Accept		No
4	TCP	0.0.0.0/0	any	10.1.66.9	http	Accept	Proxy	No
5	TCP	0.0.0.0/0	any	10.1.66.9	https	Accept	Proxy	No

Back

## Set of Rules

### General

#### A descriptive name for the set

Freely selectable name. It must clearly define the set of rules in question. A set of rules can be referred to in the incoming and outgoing rule lists using this name. To do this, the relevant name of the set of rules is selected in the *Action* column.

#### Enabled: Yes / No

Activates / deactivates the relevant set of rules.

### Firewall rules

#### Protocol

TCP, UDP, ICMP, All.

#### From IP / To IP

**0.0.0.0/0** means all IP addresses. To enter an address, use CIDR notation – see “CIDR (Classless Inter-Domain Routing)” on page 246.

#### From Port / To Port

(Only evaluated for TCP and UDP protocols)

**any** describes any selected port.

**startport:endport** (e.g. 110:120) defines a range of ports.

You can specify individual ports by giving either their port number or the corresponding service name: (e.g. 110 for pop3 or pop3 for 110).

#### Action

**Accept** means that data packets may pass through.

**Reject** means that the data packets are rejected. The sender is informed that the data packets have been rejected. In *Stealth* mode, Reject has the same effect as Drop – see below.

**Drop** means that data packets may not pass through. Data packets are discarded and the sender is not informed of their whereabouts.

**Name of set of rules**, if defined. Aside from “Accept”, “Reject” and “Drop”, the selection list also gives the names of previously defined sets of rules. If a name is selected (referred to), then the rules in this set of rules are applied here. If the rules of the set of rules applied cannot be used and put into effect with “Accept”, “Reject” or “Drop”, the rule processing continues with the rule following the one from which the set of rules was referred to.

☒ In Stealth mode, **Reject** has the same effect as **Drop**.

**Comment**

Freely selectable comment for this rule.

**Log**

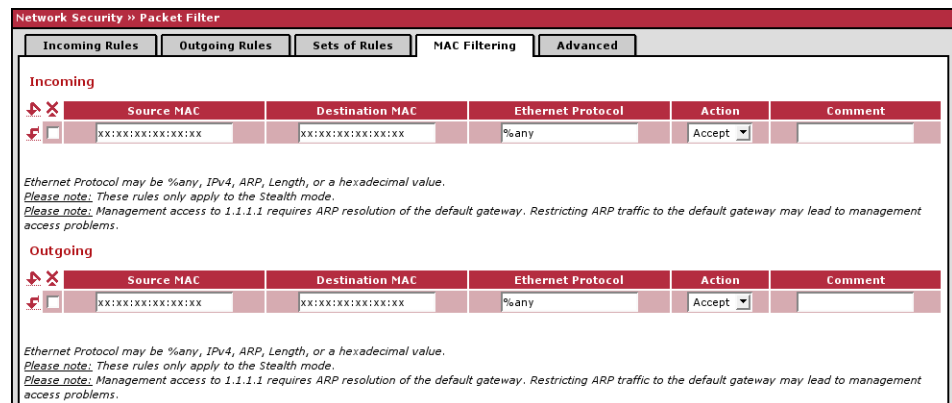
For each individual firewall rule you can specify whether the use of the rule

- should be logged (set *Log* to **Yes**) or
- should not be logged (set *Log* to **No** – factory default)

☒ Sets of rules are only used when they are referred to on the *Incoming Rules* or *Outgoing Rules* tab.

☒ Only if all the criteria of a firewall rule are fulfilled is a set of rules that is referred to in this firewall rule used.

## MAC Filtering



**Network Security » Packet Filter**

**Incoming Rules** **Outgoing Rules** **Sets of Rules** **MAC Filtering** **Advanced**

**Incoming**

Source MAC	Destination MAC	Ethernet Protocol	Action	Comment
xx:xx:xx:xx:xx:xx	xx:xx:xx:xx:xx:xx	%any	Accept	

Ethernet Protocol may be %any, IPv4, ARP, Length, or a hexadecimal value.  
 Please note: These rules only apply to the Stealth mode.  
 Please note: Management access to 1.1.1.1 requires ARP resolution of the default gateway. Restricting ARP traffic to the default gateway may lead to management access problems.

**Outgoing**

Source MAC	Destination MAC	Ethernet Protocol	Action	Comment
xx:xx:xx:xx:xx:xx	xx:xx:xx:xx:xx:xx	%any	Accept	

Ethernet Protocol may be %any, IPv4, ARP, Length, or a hexadecimal value.  
 Please note: These rules only apply to the Stealth mode.  
 Please note: Management access to 1.1.1.1 requires ARP resolution of the default gateway. Restricting ARP traffic to the default gateway may lead to management access problems.

The MAC filter is only applied to data packets that come in or go out over the ethernet port. Data packets that come in or go out over a modem connection for mGuard models with a serial port<sup>1</sup> are not picked up by the MAC filter because no ethernet protocol is used here.

Along with the packet filter (OSI layer 3/4) that filters ICMP messages and TCP/UDP connections, the mGuard can additionally be set with a MAC filter (OSI layer 2) when operating in *Stealth* mode. A MAC filter (layer 2) filters according to MAC addresses and ethernet protocols.

In contrast to the packet filter, the MAC filter is stateless. This means additional rules must be created in the opposite direction where necessary.

When no rules are defined, all ARP and IP packets are allowed.

☒ When defining MAC filter rules, pay attention to the screen display.

☒ Rules defined here have priority over packet filter rules.

### Source MAC

Definition of the source MAC address: xx:xx:xx:xx:xx:xx stands for all MAC addresses.

### Destination MAC

Definition of the destination MAC address: xx:xx:xx:xx:xx:xx stands for all MAC addresses. ff:ff:ff:ff:ff:ff is the broadcast MAC address where all ARP requests are sent.

### Ethernet Protocol

**%any** stands for all ethernet protocols. Additional protocols can be specified in name or hexadecimal value, for example:

- IPv4 or 0800
- ARP or 0806

### Action

**Accept** means that data packets may pass through.

**Drop** means that data packets may not pass through (dropped).

1. mGuard industrial RS, mGuard blade, EAGLE mGuard, mGuard delta

## Comment

Freely selectable comment for this rule.



The MAC filter does not support logging.

## Advanced

Network Security » Packet Filter	
Incoming Rules	Outgoing Rules
<b>Consistency checks</b> Maximum size of "ping" packets (ICMP Echo Request) <input type="text" value="65535"/> Enable TCP/UDP/ICMP consistency checks <input type="checkbox"/> Yes	
<b>Network Modes (Router/PPTP/PPPoE)</b> ICMP via primary external interface for the mGuard <input type="text" value="Drop"/> ICMP via secondary external interface for the mGuard <input type="text" value="Drop"/> <i>Please note: Enabling SNMP access automatically accepts incoming ICMP packets.</i>	
<b>AntiVirus Scanning</b> Connections scanned for viruses are subject to firewall rules <input type="checkbox"/> No	
<b>Stealth Mode</b> Allow forwarding of GVRP frames <input type="checkbox"/> No Allow forwarding of STP frames <input type="checkbox"/> No Allow forwarding of DHCP frames <input type="checkbox"/> Yes	
<b>Connection Tracking</b> Maximum table size <input type="text" value="4096"/> Allow TCP connections upon SYN only (after reboot connections need to be re-established) <input type="checkbox"/> No Timeout for established TCP connections <input type="text" value="432000"/> Timeout for closed TCP connections <input type="text" value="3600"/> FTP <input type="checkbox"/> Yes IRC <input type="checkbox"/> Yes PPTP <input type="checkbox"/> No H.323 <input type="checkbox"/> No SIP <input type="checkbox"/> No	

The following settings influence the basic behavior of the firewall.

## Consistency checks

### Maximum size of "ping" packets (ICMP Echo Request)

Relates to the size of the complete packet including the header. Normally the packet size is 64 bytes, although it can be larger. If oversized packets should be blocked (to prevent bottlenecks), a maximum value can be entered. This should be more than 64 bytes, as normal ICMP echo requests should not be blocked.

### Enable TCP/UDP/ICMP consistency checks: Yes / No

When this option is set to **Yes**, the mGuard performs various checks for wrong checksums, packet sizes etc. and drops packets failing the check.

The factory default for this option is **Yes**.

## Network Modes (Router/PPTP/PPPoE)

### ICMP via primary external interface for the mGuard

### ICMP via secondary external interface for the mGuard

With this option you can control which ICMP messages from the external network are accepted by the mGuard via the primary / secondary external interface. You have the following options:

**Drop:** All ICMP messages directed to the mGuard are dropped.

**Allow ping requests:** Only ping messages sent to the mGuard (ICMP type 8) are accepted.

**Allow all ICMPs:** All ICMP messages to the mGuard are accepted.

☒ Regardless of this setting, if SNMP access is enabled, incoming ICMP packets are always accepted.

## AntiVirus Scanning

### Connections scanned for viruses are subject to firewall rules: Yes / No

In the *Web Security* → *HTTP*, *Web Security* → *FTP*, *Email Security* → **POP3**, **Email Security** → **SMTP** menus, a list of server connections can be created under the *Virus Protection* tab. Files that enter mGuard via these connections are scanned for viruses (in the case of SMTP, outgoing mGuard files).

If firewall packet filters are set (*Network Security* → *Packet Filters* and/or *Network Security* → *User Firewall*) which relate to and prevent these connections, then these are only taken into consideration if the **Connections scanned for viruses are subject to firewall rules** switch is set to **Yes**.

If **No** is set (default setting), the rules that have been set for the anti-virus function have priority. Firewall packet filters that contradict them are overridden.

VPN connections are not affected as the anti-virus function is not available for VPN connections.

## Stealth Mode

### Allow forwarding of GVRP frames: Yes / No

The GARP VLAN Registration Protocol (GVRP) is used by GVRP capable switches to exchange configuration information.

When this switch is set to **Yes**, GVRP frames are allowed to traverse the mGuard in *Stealth* mode.

### Allow forwarding of STP frames: Yes / No

The Spanning Tree Protocol (STP) (802.1d) is used by bridges and switches to detect and consider loops in the network topology.

When this switch is set to **Yes**, STP frames are allowed to traverse the mGuard in *Stealth* mode.

### Allow forwarding of DHCP frames: Yes / No

When set to **Yes** the client is allowed to retrieve an IP address using DHCP independently from the firewall rules for outgoing data.

The default setting of this switch is **Yes**.

## Connection Tracking

### Maximum table size

This entry defines the upper limit. This is set to a level that can never be reached during normal operation. However, it is reached easily when attacks occur, thus giving additional protection. If special requirements are present in your operating surroundings, then you can increase this value.

**Allow TCP connections upon SYN only: Yes / No**

SYN is a special data packet in TCP/IP connections that marks the beginning of a connection attempt.

**No** (standard): The mGuard also allows connections where the beginning is not specified. This means that the mGuard can carry out a reboot during an established connection without the connection being stopped.

**Yes:** The mGuard must register the SYN packet of an existing connection. Otherwise the connection is stopped. This means that the connection is broken if the mGuard carries out a reboot during the establishment of a connection. Attacks and hijacks on existing connections are thus prevented.

**Timeout for established TCP connections**

If a TCP connection is not used after this time period, then the connection data is deleted. A connection assigned by NAT (not 1:1 NAT) must then be newly established.

The factory default is 432000 seconds (5 days).

**FTP: Yes / No**

If an outgoing connection is established to call up data during the FTP protocol, then there are two variations of data transfer. With “active FTP”, the called server establishes an additional counter-connection to the caller in order to transfer data over this connection. With “passive FTP”, the client establishes this additional connection to the server for data transfer. **FTP** must be set to **Yes** (default) so that additional connections pass through the firewall.

**IRC: Yes / No**

Similar to FTP: For IRC chat over the Internet to work properly, incoming connections must be allowed following an active connection attempt. **IRC** must be set to **Yes** (standard) for the additional connections to be passed through by the firewall.

**PPTP: Yes / No**

Must be set to **Yes** if VPN connections are established using PPTP from local computers to external computers without mGuard assistance.

The factory default for this option is **No**.

**H.323: Yes / No**

Standard: No.

Protocol used for communication meetings between two or more participants. Used for audio-visual transfers. This protocol is older than SIP.

**SIP: Yes / No**

Standard: No.

The SIP (Session Initiation Protocol) is used for communication meetings between two or more participants. Often used during IP telephony.

By selecting **Yes**, it is possible for the mGuard to monitor the SIP and add necessary firewall rules dynamically if further communication channels should be established in the same session.

When NAT is also activated, one or more locally connected computers can communicate with external computers by SIP through the mGuard.

## 6.6.2 Network Security → NAT

### Masquerading

### Network Address Translation / IP Masquerading

Lists the rules set for NAT (Network Address Translation).

For outgoing data packets, the device can rewrite the sender's IP address from its internal network to its own external address. This technique is called NAT (Network Address Translation).

This method is used whenever the internal address cannot or should not be routed externally (e.g. when a private address such as 192.168.x.x or the internal network structure should remain hidden).

This method is also known as *IP Masquerading*.

- ☒ If the mGuard is operated in *PPPoE* mode, NAT must be activated in order to gain access to the Internet. If NAT is not activated, then only VPN connections can be used.
- ☒ If more than one static IP address for the WAN port is used, the first IP address of the list is always used for IP Masquerading.
- ☒ These rules do not apply to Stealth mode.

**Factory default:** NAT is not active.

You have the following options:

#### Outgoing on Interface: External / External 2 / Any External<sup>1</sup>

Specifies over which interface the data packets go out so that the rule applies to them. **Any External** refers to the **External** and **External 2** interfaces.

#### From IP

**0.0.0.0/0** means that all internal IP addresses are subject to the NAT procedure. To enter an address, use CIDR notation – see “CIDR (Classless Inter-Domain Routing)” on page 246.

#### Comment

Can be filled with relevant comments.

### 1:1 NAT

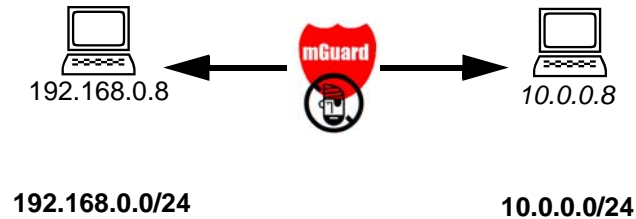
Lists the rules set for 1:1 NAT (Network Address Translation).

The mGuard mirrors addresses from the internal network to the external network.

- 
1. *External 2* and *Any External* only for devices with serial ports.  
mGuard industrial RS, mGuard blade, EAGLE mGuard, mGuard delta.  
See “Secondary external interface (= External 2)” on page 110.

Example:

The mGuard is connected to network 192.168.0.0/24 using the LAN port and to network 10.0.0.0/24 using the WAN port. By using 1:1 NAT, the LAN computer with the IP 192.168.0.8 can be reached under the IP 10.0.0.8 in the external network.



☒ 1:1 NAT cannot be used on the *External 2* interface.

☒ 1:1 NAT is only used in the *Router* network mode.

**Factory default:** NAT 1:1 is not active.

You have the following options:

**Local network**

The network address on the LAN port.

**External network**

The network address on the WAN port.

**Netmask**

The netmask as a value between 1 and 32 for the local and external network address (see also “CIDR (Classless Inter-Domain Routing)” on page 246).

**Comment**

Can be filled with relevant comments.

## Port Forwarding

Network Security » NAT

Masquerading Port Forwarding

Port Forwarding

Log ID: fw-portforwarding-No-3e8b12d3-3d40-1fd9-97e6-000cbe0220cf

No	Protocol	From IP	From Port	Incoming on IP	Incoming on Port	Redirect to IP	Redirect to Port	Comment	Log
1	TCP	0.0.0.0/0	any	%extern	http	192.168.66.1	http		No

These rules let you forward traffic targeted to the mGuard to another machine without modifying the source address.  
 The column "Incoming on IP" accepts the special value "%extern" as the mGuard's first external IP.  
 Please note: These rules won't apply to the Stealth mode.

Lists the rules set for port forwarding (DNAT = Destination NAT).

Port forwarding performs the following: The headers of incoming data packets from the external network, which are addressed to the mGuard's external IP address (or one of its external IP addresses) and to one of the ports on the mGuard, are rewritten in order to forward them to a specific port on a specific computer. In other words, both the IP address and the port number (in the header of the incoming data packets) are changed.

This method is also known as Destination NAT.

- ☒ Port forwarding cannot be used for connections initiated over the *External 2*<sup>1</sup> interface.
- ☒ The rules set here have priority over the settings made in the **Network Security, Packet Filter → Incoming Rules** menu.

### Port Forwarding

You have the following options:

#### Protocol: TCP / UDP

Enter the protocol which the rule should relate to.

#### From IP

The source address where forwarding is made.

**0.0.0.0/0** means all addresses. To enter an address, use CIDR notation – see “CIDR (Classless Inter-Domain Routing)” on page 246.

#### From Port

The source port where forwarding is made.

**any** describes any selected port.

Either the port number or the corresponding service name can be entered here (e.g. *pop3* for port 110 or *http* for port 80).

#### Incoming on IP

Enter the external IP address (or one of the external IP addresses) of the mGuard here.

OR

It cannot be specified if the destination IP address of the mGuard is assigned dynamically. In this case, use the following variable: **%extern**.

- ☒ If more than one static IP address is used for the WAN port, the variable **%extern** always corresponds to the first IP address of the address list.

1. *External 2* only for devices with serial ports.  
 See “Network → Interfaces” on page 105.

### **Incoming on Port**

The original destination port set in the incoming data packets.

Either the port number or the corresponding service name can be entered here (e.g. *pop3* for port 110 or *http* for port 80).

### **Redirect to IP**

The internal IP address to which the data packets should be forwarded.

The original destination address is overwritten with this address.

### **Redirect to Port**

The port to which the data packets should be forwarded. The original destination port will be overwritten with this port.

Either the port number or the corresponding service name can be entered here (e.g. *pop3* for port 110 or *http* for port 80).

### **Comment**

Freely selectable comment for this rule.

### **Log**

For each individual port forwarding rule you can specify whether the use of the rule

- should be logged (set *Log* to **Yes**) or
- should not be logged (set *Log* to **No** – factory default)

### 6.6.3 Network Security → DoS Protection

#### Flood Protection

Network Security » DoS Protection	
Flood Protection	
<b>TCP</b>	
Maximum number of new outgoing TCP connections (SYN) per second	75
Maximum number of new incoming TCP connections (SYN) per second	25
<b>ICMP</b>	
Maximum number of outgoing "ping" frames (ICMP Echo Request) per second	5
Maximum number of incoming "ping" frames (ICMP Echo Request) per second	3
<b>Stealth Mode</b>	
Maximum number of outgoing ARP requests or ARP replies per second (in each case)	500
Maximum number of incoming ARP requests or ARP replies per second (in each case)	500

#### TCP

##### Maximum number of new outgoing TCP connections (SYN) per second

Factory default: 75

##### Maximum number of new incoming TCP connections (SYN) per second

Factory default: 25

These two settings define upper limits for allowed incoming and outgoing TCP connections per second. These are set to a level that can never be reached during normal operation. However, they can be reached easily when attacks occur, thus giving additional protection. If special requirements are present in your operating surroundings, then these values can be increased.

#### ICMP

##### Maximum number of outgoing "ping" frames (ICMP Echo Request) per second

Factory default: 5

##### Maximum number of incoming "ping" frames (ICMP Echo Request) per second

Factory default: 3

These two settings define upper limits for allowed incoming and outgoing "ping" frames per second. These are set to a level that can never be reached during normal operation. However, they can be reached easily when attacks occur, thus giving additional protection. If special requirements are present in your operating surroundings, then these values can be increased.

## **Stealth Mode**

**Maximum number of outgoing ARP requests or ARP replies per second (in each case)**

Factory default: 500

**Maximum number of incoming ARP requests or ARP replies per second (in each case)**

Factory default: 500

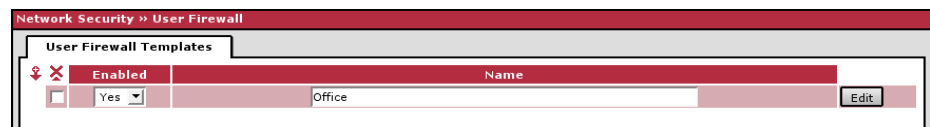
These two settings define upper limits for allowed incoming and outgoing ARP requests per second. These are set to a level that can never be reached during normal operation. However, they can be reached easily when attacks occur, thus giving additional protection. If special requirements are present in your operating surroundings, then these values can be increased.

## 6.6.4 Network Security → User Firewall

The user firewall is used exclusively by firewall users (i.e. users that are registered as firewall users – see “Authentication → Firewall Users” on page 148). Each firewall user can be assigned a set of firewall rules, also called a template.

- ☒ The anti-virus function (see “Web Security → HTTP” on page 182, “Web Security → FTP” on page 185, “Email Security → POP3” on page 188, “Email Security → SMTP” on page 191) has priority over the firewall rules defined here and can partially override them. This behavior can be overridden in the **Network Security → Packet Filters, Advanced** menu by setting the option to **Connections scanned for viruses are subject to firewall rules** – see “Advanced”, “AntiVirus Scanning” on page 170.

### User Firewall Templates



All defined user firewall templates are listed here. A template can consist of several firewall rules. A template can be assigned to several users.

#### Making a new template definition:

Click on the **Edit** button on the right side of the template table under the “(unnamed)” entry.

If the “(unnamed)” entry cannot be seen, then open a further line in the set of rules table.

#### Editing a set of rules:

Click on the **Edit** button to the right of the entry.

#### Enabled: Yes / No

Activates / deactivates the relevant template.

#### Name

Name of the template. The name is defined during creation of the template.

The *Set of Rules* page is displayed after clicking on the **Edit** button:

### User Firewall → Edit Template

After clicking on the **Edit** button, the following page appears:

## General

Network Security » User Firewall » remote service

General | Template users | Firewall rules

**Options**

A descriptive name for the template: remote service

Enabled: Yes

Comment:

Timeout: 28800

Timeout type: static

Back

## Options

### A descriptive name for the template

You can name or rename the user firewall template as desired.

### Enabled: Yes / No

When **Yes** is selected, the user firewall template becomes active as soon as firewall users log into the mGuard who are listed on the *Template users* tab (see below) and who have been assigned this template. It does not matter from which computer and under which IP address the user logs in. The assignment of user firewall rules is based on the authentication data that the user enters during login (user name, password).

### Comment

Optional: explanatory text

### Timeout

Standard: 28800.

Indicates the time in seconds at which point the firewall rules are deactivated. If the user session lasts longer than the timeout time defined here, then the user has to login again.

### Timeout type: static / dynamic

With a *static* timeout, users are logged out automatically as soon as the specified timeout expires. With a *dynamic* timeout, users are logged out automatically after all connections are closed by the user or have expired on the mGuard, and the timeout has elapsed.

An mGuard connection expires when no data is sent for the connection over the following periods:

Protocol	Connection expiration period after non-usage
TCP	5 days This value is configurable, see “Timeout for established TCP connections” on page 171. 120 additional seconds are added after connection closure. This also applies to connections closed by the user.
UDP	30 seconds after data traffic in one direction 180 seconds after data traffic in both directions
ICMP	30 seconds
Other	10 minutes

Template users

Users	
	User
<input checked="" type="checkbox"/>	Alice
<input checked="" type="checkbox"/>	Bob
<input checked="" type="checkbox"/>	Carl

Back

Users

Users

Enter the user names here. The names must correspond to those that have been defined in *Authentication* → *Firewall Users* - for more information, see “Authentication → Firewall Users” on page 148.

Firewall rules

Source IP: %authorized\_ip

Nº	Protocol	From Port	To IP	To Port	Comment	Log
<input checked="" type="checkbox"/>	TCP	any	0.0.0.0/0	http		No

Please note: If the template is configured with dynamic timeout, the logout timer will be reset to its initial value, if TCP, UDP or any other network traffic except ICMP is passing the device due to a matching user firewall rule. For a more precise description of this feature please see the user manual.

Back

Firewall rules

Source IP

The IP address from which connection establishments will be accepted. Insert the placeholder "%authorized\_ip" here if the IP address from which the user connected to the mGuard shall be used.

☒ If multiple firewall rules are defined and activated for a user, they will be searched in the order in which they are listed (top-down) until a suitable rule is found. This rule is then applied. If there are other suitable rules further down the list, then these are ignored.

You have the following options:

Protocol

All means: TCP, UDP, ICMP and other IP protocols.

From / To Port

(Only evaluated for TCP and UDP protocols)

any describes any selected port.

startport:endport (e.g. 110:120) defines a range of ports.

You can specify individual ports by giving either their port number or the corresponding service name: (e.g. 110 for pop3 or pop3 for 110).

To IP

0.0.0.0/0 means all IP addresses. To enter an address, use CIDR notation – see “CIDR (Classless Inter-Domain Routing)” on page 246.

**Comment**

Freely selectable comment for this rule.

**Log**

For each individual firewall rule you can specify whether the use of the rule

- should be logged (set *Log* to **Yes**) or
- should not be logged (set *Log* to **No** – factory default)

## 6.7 Web Security Menu (not for blade controller)

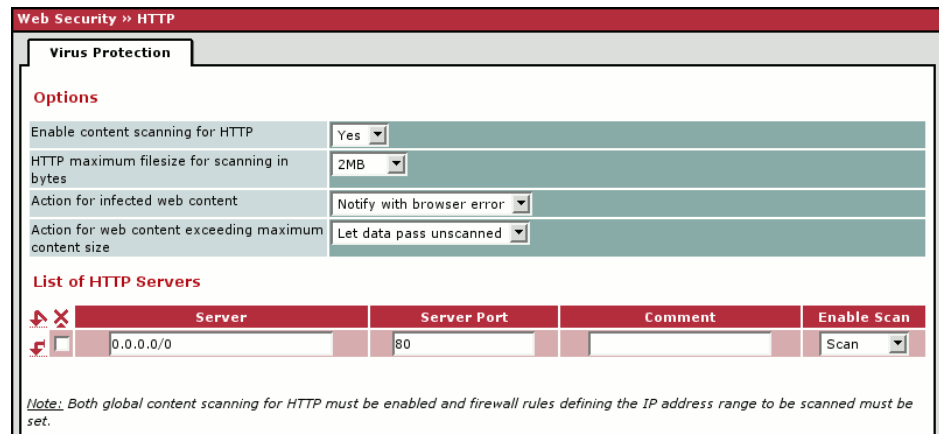
### 6.7.1 Web Security → HTTP

#### Requirements:

The following requirements must be fulfilled in order to use the virus filter:

- The anti-virus license has been installed. Instructions on how to request and install a license can be found in the section “Management → Licensing” on page 80.
- Access to an update server with the current versions of the virus signatures (see section “Management → Update” on page 82).

#### Virus Protection



**Web Security → HTTP**

**Virus Protection**

**Options**

Enable content scanning for HTTP	Yes
HTTP maximum filesize for scanning in bytes	2MB
Action for infected web content	Notify with browser error
Action for web content exceeding maximum content size	Let data pass unscanned

**List of HTTP Servers**

Server	Server Port	Comment	Enable Scan
0.0.0.0/0	80		Scan

*Note: Both global content scanning for HTTP must be enabled and firewall rules defining the IP address range to be scanned must be set.*

The HTTP protocol is used by web browsers to retrieve data from websites, but it is also used in many other applications. For example, it is used to download files (e.g. software updates) or to initialize multimedia streams.

- When virus protection is activated, the transferred file is only forwarded after it has been loaded completely and scanned. Consequently, user software may react slower when downloading larger files or whenever download speeds are slow.
- To check HTTP anti-virus protection, you can download the safe Eicar test virus which is available for test purposes at [http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm).
- The anti-virus protection is effective for HTTP connections that are established by a browser from the local network interface of the mGuard to the WAN. The anti-virus protection is not used for connections established in other directions.

#### Options

##### Enable content scanning for HTTP: Yes / No

By selecting **Yes**, files received and sent are scanned for viruses by mGuard if they are transferred via HTTP connections contained in the *List of HTTP Servers* defined below.

##### HTTP maximum filesize for scanning in bytes:

Factory default: 5 MB. Specify the maximum size of the files to be checked here. Larger files are not scanned. Depending on the “When size limit is exceeded” setting, an error message is sent to the browser if a file exceeds the size limit, or the system automatically switches to pass-through mode.

If the mGuard does not have enough memory to save a file completely or to decompress it, a corresponding error message is sent to the user's client software (browser or download manager) and an entry is written in the anti-virus log. In this case, you have the following options:

- You can try to download the file again later
- You can temporarily deactivate the virus filter for the corresponding server
- You can activate the automatic pass-through mode

### Action for infected files

#### *Notify with browser error*

An error message is sent to the HTTP client if the virus filter detects a virus in the data transferred from an HTTP server to the HTTP client. The handling of this error message depends on the respective HTTP client. A web browser will display the error message as an HTML page. If a downloaded file within an HTML page (e.g. a graphic file) is infected, then this file is not displayed in the browser. If a download manager is used to download a file via HTTP, the error message is displayed by the download manager.

### Action for files exceeding maximum message size

#### Let data pass unscanned

When this option is selected, the virus filter is switched to pass-through mode, which allows files that exceed the file size to pass through unscanned.



In this case, the data is not checked for viruses!

#### Block data

When this option is selected, the system terminates the download and sends an error message to the client software.

### List of HTTP Servers

Enter the servers where the data should be scanned for viruses.

By activating and deactivating the anti-virus function for each entry or server, you can set an exception for subsequent rules. It is also possible to enter “trusted” servers – see the example below.

Examples:

Global activation of anti-virus protection for HTTP:

 	Server	Server Port	Comment	Enable Scan
 	0.0.0.0/0	80	HTTP out to any	Scan 

Scan a subnet and exclude a “trusted” HTTP server:

 	Server	Server Port	Comment	Enable Scan
 	192.168.2.5	80	unprotected HTTP	No Scan 
 	192.168.2.0/24	80	protected HTTP	Scan 

Scan a single “untrusted” HTTP server in a subnet:

 	Server	Server Port	Comment	Enable Scan
 	192.168.2.5	80	protected HTTP	Scan 
 	192.168.2.0/24	80	unprotected HTTP	No Scan 

- ☒ To activate virus protection for HTTP or “FTP over HTTP” data traffic over a proxy, insert a new row to the list and change the default port 80 to the proxy port set in your web browser.  
Common proxy port numbers are 3128 and 8080.
- ☒ The set of rules is processed top-down, which means that the order of the rules is decisive for the results.
- ☒ The virus filter can only handle a limited number of simultaneous connections to mail, HTTP and FTP servers. If this number is exceeded, further connection attempts are refused.
- ☒ Scanning for viruses may allow outgoing connections that are usually blocked by the firewall rules defined under “Network Security → Packet Filter” and “Network Security → User Firewall”. Please see “Connections scanned for viruses are subject to firewall rules: Yes / No” on page 170 to adjust this behavior.

You have the following options:

#### **Server**

**0.0.0.0/0** means all addresses. This means that files from all HTTP servers are scanned. To enter an address, use CIDR notation – see “CIDR (Classless Inter-Domain Routing)” on page 246.

- ☒ Since a connection attempt is first handled by the mGuard, if a nonexistent server is requested (e.g. a bad IP address) the user software will act as though the connection to the server has been established, but no data has been sent. The entry of exact server addresses in the list prevents this behavior.

#### **Server Port**

Enter the number of the port for the HTTP protocol in this field. The default setting for the HTTP port is **80**.

#### **Comment**

Freely selectable comment for this rule.

#### **Scan**

##### **Scan**

The virus filter is activated for the server specified in this rule.

##### **No Scan**

The virus filter is deactivated for the server specified in this rule.

## 6.7.2 Web Security → FTP

### Requirements:

The following requirements must be fulfilled in order to use the virus filter:

- The anti-virus license has been installed. Instructions on how to request and install a license can be found in the section “Management → Licensing” on page 80.
- Access to an update server with the current versions of the virus signatures (see section “Management → Update” on page 82).

### Virus Protection

**Web Security → FTP**

**Virus Protection**

**Options**

Enable content scanning for FTP: Yes

FTP maximum filesize for scanning in bytes: SMB

Action for infected web content: Notify with browser error

Action for web content exceeding maximum content size: Let data pass unscanned

**List of FTP Servers**

Server	Server Port	Comment	Enable Scan
0.0.0.0/0	21	FTP out to any	Scan

*Note: Both global content scanning for FTP must be enabled and firewall rules defining the IP address range to be scanned must be set.*

The FTP protocol is used for uploading and downloading files.

- When virus protection is activated, the transferred file is only forwarded after it has been loaded completely and scanned. Consequently, user software may react slower when downloading larger files or whenever download speeds are slow.
- To check FTP anti-virus protection, you can download the safe Eicar test virus which is available for test purposes at [http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm).
- The mGuard can only be used to protect the FTP client.
- The anti-virus protection is effective for FTP connections that are established by an FTP client from the local network interface of the mGuard to the WAN. The anti-virus protection is not used for connections established in other directions.

### Options

#### Enable content scanning for FTP: Yes / No

By selecting **Yes**, files received and sent are scanned for viruses by mGuard if they are transferred via FTP connections contained in the *List of FTP Servers* defined below.

#### FTP maximum filesize for scanning in bytes:

Factory default: 5 MB. Specify the maximum size of the files to be checked here. Larger files are not scanned. Depending on the “When size limit is exceeded” setting, an error message is sent to the client if a file exceeds the size limit, or the system automatically switches to pass-through mode.

If the mGuard does not have enough memory to save a file completely or to decompress it, a corresponding error message is sent to the user's client software and an entry is written in the anti-virus log. In this case, you have the following options:

- You can try to download/upload the file again later
- You can temporarily deactivate the virus filter for the corresponding server
- You can activate the automatic pass-through mode

**Action for infected files****Notify with FTP error**

An error message is sent to the FTP client if the virus filter detects a virus in the data transferred from an FTP server to the FTP client. The handling of this error message depends on the respective FTP client.

**Action for files exceeding maximum message size****Let data pass unscanned**

When this option is selected, the virus filter is switched to pass-through mode, which allows files that exceed the file size to pass through unscanned.

☒ In this case, the data is not checked for viruses!

**Block data**

When this option is selected, the system terminates the download and sends an error message to the client software.

**List of FTP Servers**

Enter the servers where the data should be scanned for viruses.

By activating and deactivating the anti-virus function for each entry or server, you can set an exception for subsequent rules. It is also possible to enter “trusted” servers – see the example below.

Examples:

Global activation of anti-virus protection for FTP:

 	Server	Server Port	Comment	Enable Scan
 	0.0.0.0/0	21	FTP out to any	Scan 

Scan a subnet and exclude a “trusted” FTP server:

 	Server	Server Port	Comment	Enable Scan
 	192.168.2.5	21	unprotected FTP	No Scan 
 	192.168.2.0/24	21	protected FTP	Scan 

Scan a single “untrusted” FTP server in a subnet:

 	Server	Server Port	Comment	Enable Scan
 	192.168.2.5	21	protected FTP	Scan 
 	192.168.2.0/24	21	unprotected FTP	No Scan 

- ☒ To activate virus protection for FTP data traffic over a proxy, insert a new row to the server list and change the default port 21 to the proxy port.
- ☒ The set of rules is processed top-down, which means that the order of the rules is decisive for the results.
- ☒ The virus filter can only handle a limited number of simultaneous connections to mail, HTTP and FTP servers. Exceeding this number results in the refusal of further connection attempts.
- ☒ Scanning for viruses may allow outgoing connections that are usually blocked by the firewall rules defined under “Network Security → Packet Filter” and “Network Security → User Firewall”. Please see “Connections scanned for viruses are subject to firewall rules: Yes / No” on page 170 to adjust this behavior.

You have the following options:

**Server**

**0.0.0.0/0** means all addresses. This means files from all FTP servers are scanned. To enter an address, use CIDR notation – see “CIDR (Classless Inter-Domain Routing)” on page 246.

- ☒ Since a connection attempt is first handled by the mGuard, if a nonexistent server is requested (e.g. a bad IP address) the user software will act as though the connection to the server has been established, but no data has been sent. The entry of exact server addresses in the list prevents this behavior.

**Server Port**

Enter the number of the port for the FTP protocol in this field. The default setting for the FTP port is **21**.

**Scan**

**Scan**

The virus filter is activated for the server specified in this rule.

**No Scan**

The virus filter is deactivated for the server specified in this rule.

## 6.8 Email Security Menu (not for blade controller)

### 6.8.1 Email Security → POP3

#### Virus Protection

#### Requirements:

The following requirements must be fulfilled in order to use the virus filter:

- The anti-virus license has been installed. Instructions on how to request and install a license can be found in the section “Management → Licensing” on page 80.
- Access to an update server with the current versions of the virus signatures (see section “Management → Update” on page 82).

**Email Security » POP3**

**Virus Protection**

**Options**

Enable content scanning for POP3 (Incoming eMail)	Yes
POP3 maximum filesize for scanning in bytes	5MB
Action for infected mails	Notify email client by error message
Action for mails exceeding maximum message size	Let message pass unscanned

**Servers**

Server	Server Port	Comment	Enable Scan
0.0.0.0/0	110	POP3 out to any	Scan

*Note: Both global content scanning for POP3 must be enabled and firewall rules defining the IP address range to be scanned must be set.*

The POP3 protocol is used by the email client for incoming emails.

- The virus filter can only check unencrypted data for viruses. Therefore, encryption options such as STLS or SSL should not be activated. However, encrypted authentication using AUTH can be used, since the email itself is not encrypted.
- The anti-virus protection is effective for POP3 connections that are established by a POP3 client from the local network interface of the mGuard to the WAN. The anti-virus protection is not used for connections established in other directions.

#### Options

#### Enable content scanning for POP3 (incoming eMail): Yes / No

By selecting **Yes**, received files are scanned for viruses by mGuard if they are transferred via POP3 connections contained in the *List of POP3 Servers* defined below.

- ☒ **Tip:** When using a POP3 connection, most email clients pick up all emails during a single connection. In this case, the new settings will first take effect after the last email is collected from the server during the current connection. If settings are changed whilst an email transfer is in process, the transfer must be cancelled so the new setting can take effect.

#### POP3 maximum filesize for scanning in bytes:

Factory default: 5 MB. Specify the maximum size of the files to be checked here. Larger files are not scanned. Depending on the “When size limit is exceeded” setting, an error message is sent to the email client and the email is not received or the system automatically switches to pass-through mode.

If the mGuard does not have enough memory to save a file completely or to decompress it, a corresponding error message is sent to the user's email client software and an entry is written in the anti-virus log. In this case, you have the following options:

- You can try to download the email again later
- You can temporarily deactivate the virus filter for the corresponding server
- You can activate the automatic pass-through mode

☞ Please note that - depending on the coding scheme used – the size of the attachment may be larger than the original file.

#### **Action for infected mails**

##### **Notify recipient by email**

The recipient is informed by email if the virus filter detects a virus.

##### **Notify email client by error message**

The recipient is informed by an error message sent to the email client if the virus filter detects a virus.

☞ If the parameter “Delete received messages from server” has been set in the email client software and the “Action for infected mails” has been set to “Notify recipient by email”, the infected email is deleted on the server as the email client assumes that the email has been successfully transferred. If you do not wish to have the infected mail deleted (e.g. if you wish to download the infected email another way), only use the option “Notify email client by error message”.

#### **Action for mails exceeding maximum message size**

##### **Let message pass unscanned**

When this option is selected, the virus filter is switched to pass-through mode, which allows files that exceed the file size to pass through unscanned.

☞ In this case, the data is not checked for viruses!

##### **Block message**

When this option is selected, an error code is returned to the email client and the email is blocked.

#### **List of POP3 servers**

Enter the servers where the data should be scanned for viruses.

By activating and deactivating the anti-virus function for each entry or server, you can set an exception for subsequent rules. It is also possible to enter “trusted” servers – see the example below.

Examples:

Global activation of anti-virus protection for POP3:

 	Server	Server Port	Comment	Enable Scan
 	0.0.0.0/0	110	all outgoing connections	Scan

Scan a subnet and exclude a “trusted” POP3 server:

 	Server	Server Port	Comment	Enable Scan
 	192.168.2.5	110	unprotected POP3	No Scan
 	192.168.2.0/24	110	protected POP3	Scan

Scan a single “untrusted” POP3 server in a subnet:

 	Server	Server Port	Comment	Enable Scan
 	192.168.2.5	110	protected POP3	Scan
 	192.168.2.0/24	110	unprotected POP3	No Scan

- ☒ The set of rules is processed top-down, which means that the order of the rules is decisive for the results.
- ☒ The virus filter can only handle a limited number of simultaneous connections to mail, HTTP and FTP servers. If this number is exceeded, further connection attempts are refused.
- ☒ Scanning for viruses may allow outgoing connections that are usually blocked by the firewall rules defined under “Network Security → Packet Filter” and “Network Security → User Firewall”. Please see “Connections scanned for viruses are subject to firewall rules: Yes / No” on page 170 to adjust this behavior.

You have the following options:

#### Server

**0.0.0.0/0** means all addresses. This means that files from all POP3 servers are scanned. To enter an address, use CIDR notation – see “CIDR (Classless Inter-Domain Routing)” on page 246.

- ☒ Since a connection attempt is first handled by the mGuard, if a nonexistent server is requested (e.g. a bad IP address) the user software will act as though the connection to the server has been established, but no data has been sent. The entry of exact server addresses in the list prevents this behavior.

#### Server Port

Enter the number of the port for the POP3 protocol in this field. The default setting for the POP3 port is **110**.

#### Comment

Freely selectable comment for this rule.

#### Scan

##### Scan

The virus filter is activated for the server specified in this rule.

##### No Scan

The virus filter is deactivated for the server specified in this rule.

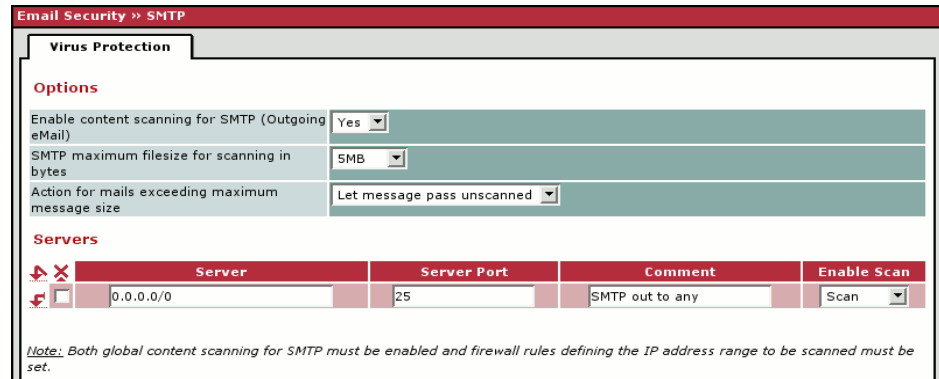
## 6.8.2 Email Security → SMTP

### Virus Protection

#### Requirements:

The following requirements must be fulfilled in order to use the virus filter:

- The anti-virus license has been installed. Instructions on how to request and install a license can be found in the section “Management → Licensing” on page 80.
- Access to an update server with the current versions of the virus signatures (see section “Management → Update” on page 82).



The SMTP protocol is used by the email client or Mail Transfer Agent (MTA) for sending emails.

- The virus filter can only check unencrypted data for viruses. Therefore, encryption options such as TLS should not be activated. If a virus or error is detected, a corresponding error code is sent to the email client software and an entry is written in the anti-virus log. The intended recipient will receive neither the infected mail nor notification of it.
- The anti-virus protection is effective for SMTP connections that are established by a mail client or mail server from the local network interface of the mGuard to the WAN. The anti-virus protection is not used for connections established in other directions.

### Options

#### Enable content scanning for SMTP (Outgoing eMail): Yes / No

By selecting **Yes**, outgoing files are scanned for viruses by mGuard if they are transferred via SMTP connections contained in the *List of SMTP Servers* defined below.

#### SMTP maximum filesize for scanning in bytes:

Factory default: 5 MB. Specify the maximum size of the files to be checked here. Larger files are not scanned. Depending on the “When size limit is exceeded” setting, an error message is sent to the SMTP client and the email is not sent, or the system automatically switches to pass-through mode.


If the mGuard does not have enough memory to save a file completely or to decompress it, a corresponding error message is sent to the user's email client software and an entry is written in the anti-virus log. In this case, you have the following options:

- You can try to send the file again later
- You can temporarily deactivate the virus filter for the corresponding server
- You can activate the automatic pass-through mode

☞ Please note that – depending on the coding scheme used – the size of the attachment may be larger than the original file.

**Action for mails exceeding maximum message size****Let message pass unscanned**

When this option is selected, the virus filter is switched to pass-through mode, which allows files that exceed the file size to pass through unscanned.

 In this case, the data is not checked for viruses!

**Block message**

When this option is selected, an error code is returned to the email client and the email is blocked.

**List of SMTP Servers**

Enter the servers where the data should be scanned for viruses.

By activating and deactivating the anti-virus function for each entry or server, you can set an exception for subsequent rules. It is also possible to enter “trusted” servers – see the example below.

Examples:

Global activation of anti-virus protection for SMTP:

 	Server	Server Port	Comment	Enable Scan
 	0.0.0.0/0	25		Scan 

Scan a subnet and exclude a “trusted” SMTP server:

 	Server	Server Port	Comment	Enable Scan
 	192.168.2.5	25	server with own AV engine	No Scan 
 	192.168.2.0/24	25	attackable server	Scan 

Scan for a single SMTP server in a subnet:

 	Server	Server Port	Comment	Enable Scan
 	192.168.2.5	25	weak SMTP server	Scan 
 	192.168.2.0/24	25	servers with own AV engine	No Scan 

- ☒ The set of rules is processed top-down, which means that the order of the rules is decisive for the results.
- ☒ The virus filter can only handle a limited number of simultaneous connections to mail, HTTP and FTP servers. If this number is exceeded, further connection attempts are refused.
- ☒ Scanning for viruses may allow outgoing connections that are usually blocked by the firewall rules defined under “Network Security → Packet Filter” and “Network Security → User Firewall”. Please see “Connections scanned for viruses are subject to firewall rules: Yes / No” on page 170 to adjust this behavior.

You have the following options:

**Server**

**0.0.0.0/0** means all addresses. This means that files to all SMTP servers are scanned. To enter an address, use CIDR notation – see “CIDR (Classless Inter-Domain Routing)” on page 246.

- ☒ Since a connection attempt is first handled by the mGuard, if a nonexistent server is requested (e.g. a bad IP address) the user software will act as though the connection to the server has been established, but no data has been sent. The entry of exact server addresses in the list prevents this behavior.

**Server Port**

Enter the number of the port for the SMTP protocol in this field.  
The default setting for the SMTP port is **25**.

**Comment**

Freely selectable comment for this rule.

**Scan**

**Scan**

The virus filter is activated for the server specified in this rule.

**No Scan**

The virus filter is deactivated for the server specified in this rule.

## 6.9 IPsec VPN Menu (not for blade controller)

### 6.9.1 IPsec VPN → Global

#### Options

IPsec VPN → Global

Options

DynDNS Monitoring

Options

Allow packet forwarding between VPN connections

No

Start and stop the specified VPN connection with the CMD contact and signal the status of the connection with the ACK contact.

Off

As long as no VPN connection is configured the only choice is "Off".

Switch type connected to the CMD contact

Push button

IP Fragmentation

Some routers fail to forward large UDP packets which may break the IPsec protocol. The following options allow you to reduce the size of the UDP packets generated by IPsec to traverse such routers.

IKE Fragmentation

The IKE Main Mode with X.509 certificates usually generates large UDP packets. With this option enabled, IKE Main Mode packets will be fragmented within the IKE protocol itself and thereby avoid large UDP packets.

Yes

IPsec MTU (default is 16260)

The internal IPsec MTU is usually set to a large value like 16260 to avoid fragmentation of IP packets within IPsec. When IPsec has to traverse NAT routers, encrypted IP packets will be transferred via UDP. By reducing the IPsec MTU, the IP packets will be fragmented before they are encapsulated in UDP and thereby avoid large UDP packets. A recommended value in such situations is 1414 or smaller.

16260

#### Options

#### Allow packet forwarding between VPN connections: Yes / No

**No** (standard): VPN connections exist separately.

**Yes:** Hub and Spoke feature activated: A control center diverts VPN connections to several branches, who can also communicate with each other. mGuard remote peers can also exchange data between each other during the establishment of such a star VPN connection topology. In this case, we recommend that the local mGuard consults CA certificates for the authentication of remote peers – see “Authentication” on page 207.

- ☞ The **Yes** setting is only needed for mGuards communicating between two different VPN remote peers.
- ☞ The local network of the communicating mGuard must be configured so that the remote networks containing the VPN remote peers are included. This is necessary for the correct communication between two VPN remote peers. The opposite set-up (local and remote network interchanged) must also be established for VPN remote peers. See the example in the figure on Page 203.
- ☞ The **Yes** setting is not supported in the *Stealth* network mode.

Only for  
mGuard industrial RS

#### Start and stop the specified VPN connection with the CMD contact...: **Off / VPN connection name**

The mGuard industrial RS has connections where an external push button or On/Off switch and a signal LED can be connected. A defined VPN connection can be established or terminated using the push button or the On/Off switch. The VPN connection in question is defined here:

If VPN connections are defined and listed under the IPsec VPN → Connections menu (see “IPsec VPN → Connections” on page 198), then these are displayed in the selection list. If you want the connection to be established or terminated manually by pressing the button or using the switch, then you select this here.

- ☞ Starting and stopping a connection using a push button/switch only makes sense if this connection is configured as follows: The connection is disabled (**Enabled:** No) or **Connection startup** is set to “Wait”. Otherwise, the connection to the mGuard is established independently.

When **Off** is selected, this function is disabled. If a push button or On/Off switch is connected to the mGuard service contacts, then using it has no effect.

---

Only for  
mGuard industrial RS

---

#### Switch type connected to the CMD contact: Push button / On/off switch

The mGuard industrial RS has connections where an external push button/switch and a signal LED can be connected. Select the switch type that is connected to the corresponding service contacts of the mGuard industrial RS. See also “Installing the mGuard industrial RS” on page 24 under **Service Contacts**. How to operate the different switch types is also described here.

- ☞ If a VPN connection is established by operating the push button or switch, the connection remains in place until it is terminated by operating the push button/switch again.
- ☞ If an On/Off switch is used (instead of a push button) and it is operated to establish a VPN connection, this connection is re-established automatically when the mGuard is restarted.

## IP fragmentation

### IKE fragmentation: Yes / No

UDP packages can be oversized if an IPsec connection is made between the participants, including the exchange of certificates. Some routers are not capable of forwarding large UDP packages if they are fragmented during the transfer process (e.g. by DSL in 1500 byte segments). Some defective devices forward the first fragment only, leading to a connection failure.

If two mGuards communicate with each other, then the dispatch of small UDP packages should be agreed upon first. This prevents packages from being fragmented during transportation, which may lead to incorrect transfer from certain routers.

If you want to use this option, then set it to **Yes**.

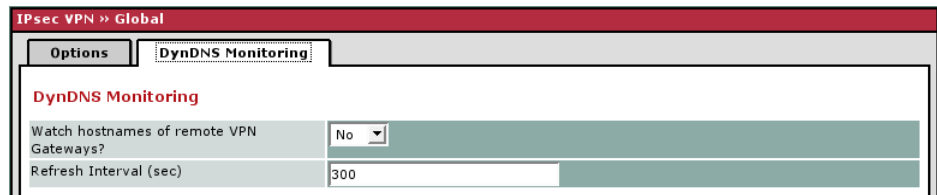
- ☒ If **Yes** is selected, then the setting only comes into effect when the remote peer is an mGuard with installed firmware above version 5.1.0. In all other cases the setting has no effect (also no negative effects).

**MTU for IPsec (factory default of 16260)**

The methods for avoiding oversized IKE data packages (incorrect transfer) can also be applied for IPsec data packages. In order to remain below the upper limit set by DSL (1500 bytes), we recommend setting a value of 1414 (bytes). This also allows enough space for additional headers.

If you want to use this option, then set the value lower than 16260.

## DynDNS Monitoring



The screenshot shows the 'IPsec VPN >> Global' configuration page. Under the 'Options' tab, the 'DynDNS Monitoring' sub-tab is selected. The 'DynDNS Monitoring' section contains two settings: 'Watch hostnames of remote VPN Gateways?' set to 'No' and 'Refresh Interval (sec)' set to '300'.

IPsec VPN >> Global	
Options   DynDNS Monitoring	
<b>DynDNS Monitoring</b>	
Watch hostnames of remote VPN Gateways?	No
Refresh Interval (sec)	300

See below for an explanation of DynDNS: Services → DynDNS Registration.

### DynDNS Monitoring

#### Watch hostnames of remote VPN Gateways? Yes / No

If the mGuard has been given the address of the remote VPN gateway as a hostname (see “Defining VPN connection / VPN connection channels” on page 200) and this hostname is registered with a DynDNS Service, then the mGuard can check the DynDNS at regular intervals for whether any changes have occurred. If so, the VPN connection will be setup to the new IP address.

#### Refresh Interval (seconds)

Standard: 300

## 6.9.2 IPsec VPN → Connections

Requirements for a VPN connection:

The main requirement for a VPN connection is that the IP addresses of the VPN partners are known and accessible.

- In order for an IPsec connection to be setup successfully, the VPN remote peer must support IPsec with the following configuration:
  - Authentication via Pre-Shared Key (PSK) or X.509 certificate
  - ESP
  - Diffie-Hellman Groups 2 and 5
  - DES, 3DES or AES encryption
  - MD5 or SHA-1 hash algorithms
  - Tunnel or Transport Mode
  - Quick Mode
  - Main Mode
  - SA Lifetime (1 second to 24 hours)

If the remote peer system is running Windows 2000, the *Microsoft Windows 2000 High Encryption Pack* or at least *Service Pack 2* must be installed.

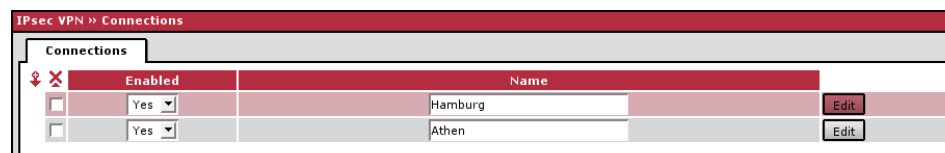
- If the remote peer is behind a NAT router, the peer must support NAT-T. Alternatively, the NAT router must support the IPsec protocol (IPsec/VPN Passthrough). For technical reasons only IPsec Tunnel connections are supported in both cases.

### Connections

Lists the VPN connections that have been defined.

Each entry listed here can identify an individual VPN connection or a group of VPN connection channels. You have the possibility of defining several tunnels under the transport or tunnel settings of the respective entry.

You also have the possibility of defining, activating and deactivating new VPN connections, changing (editing) the VPN or connection group settings and deleting connections.



IPsec VPN » Connections			
Connections			
	Enabled	Name	
<input type="checkbox"/>	Yes	Hamburg	Edit
<input type="checkbox"/>	Yes	Athen	Edit

### Making a new definition of VPN connection / VPN connection channels:

Click on the **Edit** button on the connection table under the “(unnamed)” entry.

If the “(unnamed)” entry cannot be seen, then open a further line in the table.

### Editing VPN connection / VPN connection channels:

Click on the **Edit** button to the right of the entry.

**URL for starting, stopping and status query of a VPN connection**

The following URL can be used to start and stop VPN connections and query the connection status, independently from their **Enabled** setting:

`https://server/nph-vpn.cgi?name=verbindung&cmd=(up/down/status)`

Example:

```
wget https://admin:mGuard@192.168.1.1/nph-vpn.cgi?name=Athen&cmd=up
```

A command like this relates to all connection channels that are summarized under the respective name (in this example, *Athen*). This is the name entered under “A descriptive name for the connection” on the *General* tab. If ambiguity occurs, then the URL call only affects the first entry in the connections list.

Access to individual VPN connection channels is not possible. If individual channels are deactivated (**Active:** No), then these are not started. In this way, starting and stopping have no effect on the settings of the individual channels (i.e. the list under *Transport and Tunnel Settings*).

Starting and stopping a connection using a URL only makes sense if the configuration of the connection is deactivated (**Active:** No) or when **Connection startup** is set to “Wait”. Otherwise, the connection to the mGuard is established independently.

If the status of a VPN connection is queried using the URL detailed above, then the following answers can be expected:

Answer	Meaning
<b>unknown</b>	A VPN connection with this name does not exist.
<b>void</b>	The connection is inactive due to an error (e.g. the external network is down or the hostname of the remote peer could not be resolved in an IP address (DNS)).
<b>ready</b>	The connection is ready to establish channels or allow incoming queries regarding channel set-up.
<b>active</b>	At least one channel is set-up for the connection.

### 6.9.3 Defining VPN connection / VPN connection channels

The following page appears after you click the **Edit** button, depending on the mGuard network mode (for *Stealth* and *Router* modes see “Network → Interfaces” on page 105):

#### General

Only in Stealth mode

#### Options

##### A descriptive name for the connection

You can name or rename the connection as desired. If several connection channels are defined below under *Transport and Tunnel Settings*, then this name applies to the whole set of VPN connection channels summarized under this name.

Similarities between VPN connection channels:

- Same authentication procedure, as defined under the *Authentication* tab (see “Authentication” on page 207)
- Same firewall settings
- Same IKE option settings

##### Enabled: Yes / No

Defines whether the VPN connection channels should be completely active (Yes) or not (No).

##### Address of the remote site's VPN gateway

An IP address, hostname or **%any** for several remote peers or remote peers behind a NAT router.



The address of the gateway to the private network where the remote communication partner can be found.

- If the mGuard should actively initiate and set up the connection to the remote peer, enter the IP address or the hostname of the remote peer here.
- If the remote peer VPN gateway does not have a fixed and known IP address, you can use the DynDNS Service (see glossary) to simulate a fixed and known address.
- If the mGuard should be ready to accept a connection that was actively initiated and set up by a remote peer with any IP address, enter: **%any**

This setting should also be selected for VPN star configurations when the mGuard is connected to the control center.

The mGuard can then be “called” by a remote peer that has been dynamically assigned its IP address by the ISP (i.e. it has a changeable IP address). In this scenario, you may only enter an IP address when the remote peer has a fixed and known IP address.

☒ **%any** can only be used along with the authentication procedure using X.509 certificates.

☒ If locally stored CA certificates are to be used to authenticate the remote peer, the address of the remote peer's VPN gateway can be entered explicitly (via IP address or hostname) or via **%any**. If it is entered using an explicit address (and not with “%any”), then a VPN identifier (see “VPN Identifier” on page 212) must be specified.

☒ **%any** must be selected when the remote peer is located behind a NAT gateway. Otherwise the renegotiation of new connection keys will fail after the connection is established.

### Connection startup: Initiate / Initiate on traffic / Wait

#### Initiate

The local mGuard sets up the connection to the remote peer. In the *Address of the remote site's VPN gateway* (see above), the fixed remote peer IP address or domain name must be entered.

#### Initiate during data traffic

The connection is initiated automatically when the mGuard sees that the connection should be used (can be selected in all operating modes of the mGuard (*Stealth*, *Router* etc.)).

#### Wait

The local mGuard is ready to accept connections which a remote peer actively initiates and sets up to the local mGuard.

☞ When **%any** is entered under *Address of the remote site's VPN gateway*, then **Wait** must be selected.

### Transport and Tunnel Settings

Stealth mode:

Transport and Tunnel Settings

Enabled	Type	Local	Remote	Virtual IP	More...
<input checked="" type="checkbox"/> Yes	Tunnel	192.168.1.1/32	192.168.254.1/32	192.168.1.1	More...

Click here when further tunnel or transport paths should be specified.

Router mode:

Transport and Tunnel Settings

Enabled	Type	Local	Remote	More...
<input checked="" type="checkbox"/> Yes	Transport	192.168.1.1/32	192.168.254.1/32	More...

### VPN connection channels

A VPN connection defined under a descriptive name can consist of more than one VPN connection channel. Therefore you can define multiple VPN connection channels here.

### For each individual VPN connection channel

After the **More...** button is clicked, another partially overlapping page is displayed where connection parameters can be defined for the relevant transport path or tunnel.

#### Enabled: Yes / No

You specify whether the connection channel should be active (Yes) or not (No).

#### Comment

Freely selectable comments. Can be left empty.

#### Type

The following can be selected:

- Tunnel (Network ↔ Network)
- Transport (Host ↔ Host)

#### Tunnel (Network ↔ Network)

This connection type is suitable in all cases and is also the most secure. In this mode, the IP datagrams are completely encrypted with a new header and sent to the remote peer VPN gateway – the “tunnel end”. The transferred datagrams are then decrypted and the original datagrams are restored. These are then forwarded to the destination system.

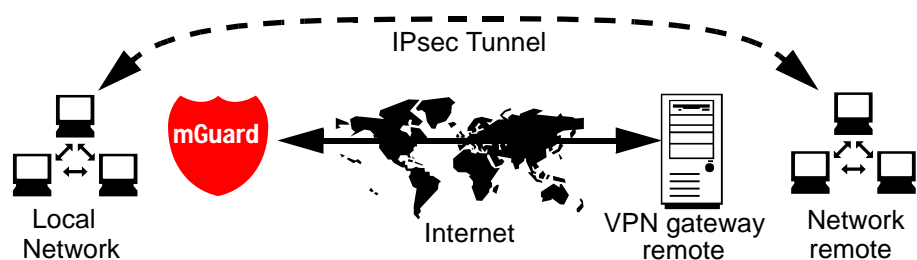
#### Transport (Host ↔ Host)

In this type of connection, the device only encrypts the data of the IP packets. The IP header information remains unencrypted.

When a change to *Transport* is made, the following fields (apart from the protocol) are hidden as these parameters are omitted.

#### Local / remote – for connection type *Tunnel* (Network ↔ Network)

Define the network areas for both tunnel ends under **Local** and **Remote**.



#### Local

Enter the network or computer address where the local mGuard is connected.

## Remote

Enter the network or computer address found behind the remote VPN gateway.

If the address of the *remote site's VPN gateway* (See “Address of the remote site's VPN gateway” on page 200) is entered as **%any**, it is possible that a number of different remote peers will connect to the mGuard.

### Default route over the VPN:

The address 0.0.0.0/0 provides a *Default route over the VPN*.

In this case, all data traffic where no other tunnel or route exists is forwarded through this VPN tunnel.

- ☒ A default route over the VPN should only be given for a single tunnel.
- ☒ *Default route over the VPN* cannot be used in *Stealth* mode.

## Options following installation of a VPN tunnel group license

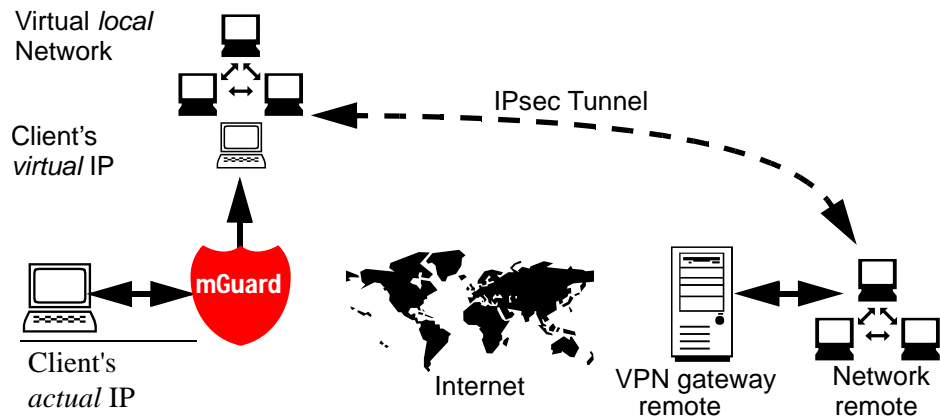
If the address of the *remote site's VPN gateway* is entered as **%any**, it is possible that there are many mGuards or many networks on the remote site. Then a very large address range is specified in the **Remote** field for the local mGuard, and a part of this address range is used on the remote mGuards for the network entered for each of them under **Local**. This is illustrated as follows: The entries in the *Local* and *Remote* fields for the local and remote mGuards could be made as follows:

Central mGuard			Branch mGuard <b>A</b>	
Local	Remote		Local	Remote
10.0.0.0/8	10.0.0.0/8	>	10.1.7.0/24	10.0.0.0/8
			Branch mGuard <b>B</b>	
			Local	Remote
		>	10.3.9.0/24	10.0.0.0/8
			etc.	

In this way, configuring a single tunnel can allow you to establish connections for a number of peers.

- ☒ To use this option, the *VPN tunnel group license* must be installed, unless the device was delivered accordingly. The system must be rebooted in order to use this installed license.

**Virtual IP** (*only in Stealth mode*)



In *Stealth* mode the VPN local network is simulated by the mGuard. Within this *virtual* network, the client is known and accessible under the *virtual* IP address entered here.

→ Further settings can be made by clicking “More...”

- - Connection type *Tunnel*

IPsec VPN » Connections » ... » Tunnel Settings

**General**

**Options**

Enabled	Yes
Comment	
Type	Tunnel
Local	192.168.1.1/32
Remote	192.168.254.1/32

**1-to-1 NAT**

Enable 1-to-1 NAT of the local network to an internal network	No
Enable 1-to-1 NAT of the remote network to a different network	No

**Protocol**

Protocol	All
----------	-----

[Back](#)

## General

### Options

**Enabled: Yes / No**

As above.

**Comment**

Freely selectable comments. Can be left empty.

**Type: Tunnel / Transport**

As above. When a change to *Transport* is made, the following fields (apart from the *protocol*) are hidden as these parameters are omitted.

**Local**

As above.

**Remote**

As above.

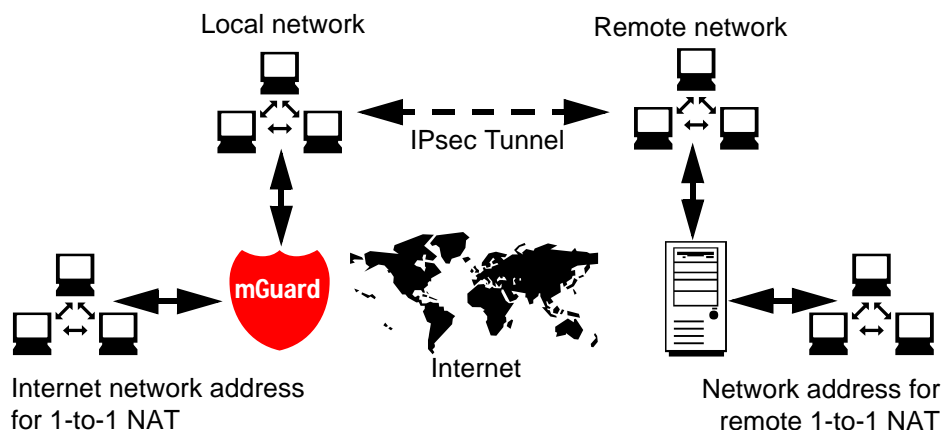
**Virtual IP for the client**

As above (previous page).

### 1-to-1 NAT

Only in Router mode

With 1-to-1 NAT it is still possible to enter the used network addresses (local and/or remote) for specifying the tunnel beginning and end, independently of the tunnel parameters agreed with the remote peer:



**Enable 1-to-1 NAT of the local network to an internal network: Yes / No**

Rewrites the local network specified under *Local* to an existing local network.  
The default setting is **No**.

**Internal network address for 1-to-1 NAT**

(Only when **Yes** is selected above)

The actual network address of the system in the local network.  
The netmask is taken from the *Local* field.

**Enable 1-to-1 NAT of the remote network to a different network**

Rewrites the remote network agreed by the VPN remote peer under *Remote* as if the computer connected there with the addresses was in another network.  
The default setting is **No**.

**Network address for remote 1-to-1 NAT**

(Only when **Yes** is selected above)

The remote network address actually addressed by the systems in the local network.  
The netmask is taken from the *Remote* field.

☒ If the *remote network* or the *remote network for 1-to-1 NAT* are within one of the networks directly connected to the mGuard LAN port, then the mGuard will additionally answer ARP requests for IP addresses within the remote network.

This allows access to a remote VPN using local IP addresses without changing the routing of locally connected clients.

**Protocol****Protocol: All / TCP / UDP / ICMP**

Select whether the VPN is restricted to a certain protocol or it is valid for all data traffic.

**TCP or UDP:**

Protocol	TCP
Local Port ( '%all' for all ports, a number between 1 and 65535 or '%any' to accept any proposal.)	%all
Remote Port ( '%all' for all ports, a number between 1 and 65535 or '%any' to accept any proposal.)	%all

**Local Port**

**%all** (standard) specifies that all ports can be used. If a specific port should be used, then enter the port number. **%any** specifies that port selection is made by the client.

**Remote Port**

**%all** (standard) specifies that all ports can be used. If a specific port should be used, then enter the port number.

## Tunnel settings IPsec / L2TP

If clients should connect to the mGuard by IPsec/L2TP, then activate the L2TP server and make the following entries in the fields specified below:

**Type:** Transport

**Protocol:** UDP

**Local Port:** %any

**Remote Port:** %any

## Authentication

**IPsec VPN » Connections » Berlin**

**General | Authentication | Firewall | IKE Options**

**Authentication**

Authentication method: X.509 Certificate

Local X.509 Certificate: None

Remote CA Certificate: No CA certificate, but the Remote Certificate below

Remote Certificate: No Certificate installed

Filename (\*.pem):  Browse... Upload

**VPN Identifier**

Local: Valid values are:  
• the certificates distinguished name (same as no entry)

Remote: Valid values are:  
• the certificates distinguished name (same as no entry)  
error: failed to read X509 file

Back

## Authentication

### Authentication method

The following two possibilities are available:

- X.509 Certificate (standard)
- Pre-Shared Key

Depending on the chosen option, the page has different setting possibilities.

### ➔ Authentication method: X.509 Certificate

This method is supported by most modern IPsec implementations. Each VPN participant possesses a secret private key, plus a public key in the form of an X.509 certificate. This contains further information on the owner and Certificate Authority (CA).

The following aspects must be defined:

- a) How the local mGuard authenticates itself to the remote peer
- b) How the local mGuard authenticates the remote peer

**Authentication**

Authentication method: X.509 Certificate

Local X.509 Certificate: VPN terminal service London

Remote CA Certificate: VPN-SubCA 01

Remote Certificate: No Certificate installed

Filename (\*.pem):  Browse... Upload


## → a) How the local mGuard authenticates itself to the remote peer

### Local X.509 Certificate

Defines which machine certificate the mGuard uses as authentication to the VPN remote peer.

Select one of the machine certificates from the selection list.

The selection list gives a selection of machine certificates that are loaded in the mGuard under the *Authentication → Certificate* menu – see “Authentication → Certificates” on page 150 of this manual.

 If *None* is displayed, then a certificate must be installed first. The *None* entry must not be left in place, as this results in no X.509 authentication.

## → b) How the local mGuard authenticates the remote peer



The following definition relates to how the mGuard verifies the authentication of the VPN remote peer.

The table below shows which certificates must be provided for the mGuard to authenticate the VPN remote peer if the peer displays one of the following certificate types on connection:

- A machine certificate signed by a CA
- A self-signed machine certificate

For further information on the following table see chapter “6.5.3 Authentication → Certificates” on page 150.

### Authentication for VPN

The remote peer shows the following:	Machine certificate signed by CA	Machine certificate self-signed
The mGuard authenticates the remote peer using:		
	Remote Certificate  OR  All CA certificates that build the chain to the root CA certificate together with the certificates displayed by the remote peer	Remote certificate

According to this table, certificates must be provided that the mGuard has to use for authentication of the respective VPN remote peer.

The following instructions assume that the certificates have been correctly installed in the mGuard. See “6.5.3 Authentication → Certificates” on page 150 (except remote certificate – see below).

- ☒ If the use of block lists (CRL checking) is activated under the *Authentication → Certificate, Certificate settings* menu, then each certificate signed by a CA that shows a VPN remote peer is checked for blocks. Locally configured remote certificates (imported here) are excepted.

### Remote CA Certificate

- ➔ When the VPN remote peer authenticates itself with a **self-signed** machine certificate.

In this case select:

***Remote certificate below, not CA certificate***

The certificate is then installed under *Remote Certificate*.

- ☞ It is not possible to refer to a remote certificate loaded in the *Authentication → Certificates* menu.

- ➔ When the VPN remote peer authenticates itself with a machine certificate **signed by a CA**:

It is possible to authenticate the machine certificate shown by the remote peer as follows:

- A Using a CA certificate
- B Using the relevant remote certificate

#### A Using a CA certificate

Only the CA certificate from the CA that signed the certificate shown by the VPN remote peer should be referred to here (selection from list). The further CA certificates that build the chain to the root CA certificate together with the certificate shown by the remote peer must be installed in the mGuard under *Authentication → Certificates*.

The selection list gives a selection of all CA certificates that are loaded in the mGuard under the *Authentication → Certificate* menu.

Further possibility:

***All known CAs***

With this setting, all VPN remote peers are accepted, providing that they log on with a certificate signed by a recognized Certificate Authority (CA).

The CA is recognized when the relevant CA certificate and all other CA certificates are stored in the mGuard. These then build the chain to the root certificate together with the certificates shown.

#### B Using the relevant remote certificate

Select the following entry from the list:

***Remote certificate below, not CA certificate***

The certificate is then installed under *Remote Certificate*.

- ☞ It is not possible to refer to a remote certificate loaded in the *Authentication → Certificates* menu.

### Remote Certificate

Must be configured if the VPN remote peer is authenticated using a remote certificate.

To import a certificate, please proceed as follows:

#### Requirement:

The certificate file (file format = \*.pem, \*.cer or \*.crt) is saved on the connected computer.

Proceed as follows:

1. Click on **Browse...** to select the file.
2. Click on **Upload**.  
The certificate contents are then displayed.

### VPN Identifier

The following explanation applies when authentication of the VPN remote peer is made using CA certificates.

VPN gateways use the VPN Identifier to recognize which configurations belong to the same VPN connection.

If the mGuard consults CA certificates to authenticate a VPN remote peer, then it is possible to use the VPN Identifier as a filter. To do this, make the appropriate entries in the *Remote peer* text field.

- ☒ If the address of the *remote site's VPN gateway* (see Page 200) is entered using an explicit address (and not with “%any”), then a VPN identifier must be specified under *Remote*.

### Local

Standard: Empty

You can specify the name that the mGuard uses to identify itself to the remote peer using the VPN Identifier. This must match the entries in the mGuard machine certificate.

Valid entries are:

- Empty (i.e. no entry) (standard). The subject entry of the machine certificate (earlier known as *Distinguished Name*) is then used.
- Subject entry in machine certificate
- One of the *Subject Alternative Names* listed in the certificate. When the certificate contains *Subject Alternative Names*, these are entered under “Valid entries are:”. These can be IP addresses, hostnames with preset @-signs or email addresses.

**Remote peer**

Defines what must be entered as a subject in the VPN remote peer machine certificate for the mGuard to accept this VPN remote peer as a communication partner.

It is then possible to limit or grant access by VPN remote peers that would accept the mGuard in principle based on the certification check:

- Limitation to certain *subjects* (i.e. machines) or to *subjects* that have certain attributes

OR

- Grant for all *subjects*

(See also glossary under “Subject, certificate”.)

☞ “Subject” was previously known as “Distinguished Name”.

**Grant for all subjects:**

If the *Remote peer* field is left empty, then any subject entries are allowed in the machine certificate displayed by the VPN remote peer. Identification or definition of the subject in the certificate is then no longer needed.

**Limitation to certain subjects:**

In the certificate, the certificate owner is entered in the *Subject* field.

The entry is comprised of several attributes. These attributes are either expressed as an Object Identifier (e.g.: 132.3.7.32.1) or, more commonly, as an abbreviation with a relevant value.

Example: CN=VPN end point 01, O=Smith and Co., C=UK

If certain subject attributes have very specific values for the acceptance of the VPN remote peer by the mGuard, then these must be specified accordingly. The values of the other freely selectable attributes are entered using the \* wildcard.

Example: CN=\*, O=Smith and Co., C=UK

(with or without spaces between attributes)

In this example, the attribute (C=UK and O=Smith and Co.) must be entered in the certificate under “subject”. Only then does the mGuard accept the certificate owner (subject) as a communication partner. The other attributes in the certificates to be filtered can have freely selectable values.

☞ If a subject filter is set, the number and sequence of the entered attributes must correspond to those of the certificates where the filter is used.

Pay attention to capitalization.

## ➔ Authentication method: Pre-Shared Secret (PSK)

The screenshot shows the configuration page for an IPsec VPN connection named 'London'. The 'Authentication' tab is active. In the 'Authentication' section, the 'Authentication method' is set to 'Pre-Shared Secret (PSK)' and the 'Pre-Shared Secret Key (PSK)' is 'complicated\_like\_5Dy0qoD\_and\_long'. In the 'VPN Identifier' section, there are two fields: 'Remote' and 'Local'. Both fields have a text box and a help message: 'By default the IP address of the peer is used. Other possible settings are a hostname ("@hostname") or an e-mail address ("name@hostname").'

This method is mainly used by older IPsec implementations. In this case both sides of the VPN authenticate themselves with the same PSK.

To make the agreed key available to the mGuard, proceed as follows:

Enter the agreed character string in the **Pre-Shared Secret Key (PSK)** entry field.

To achieve security comparable to that of 3DES, the string should consist of about 30 randomly selected characters, and should include upper and lower case characters and digits.

- ☒ The *Pre-Shared Secret Key* cannot be used with dynamic (%any) IP addresses. Only fixed IP addresses or hostnames at both ends are supported. However, changing IP addresses (DynDNS) can be hidden behind the hostnames.
- ☒ *Pre-Shared Secret Key* cannot be used when one (or both) of the communication partners is found behind a NAT gateway.

## VPN Identifier

VPN gateways use the *VPN Identifier* to recognize which configurations belong to the same VPN connection.

The following entries are valid for PSK:

- Empty (IP address used as default)
- An IP address
- A hostname with prefixed “@” symbols (e.g. “@vpn1138.example.com”)
- An email address (e.g. “piepiorra@example.com”)

## Firewall

IPsec VPN » Connections » New York

General Authentication **Firewall** IKE Options

**Incoming**

Log ID: fw-vpn-v000\_000-in-Nº-3e8b12c4-3d40-1fd9-97e6-000cbe0220cf

No	Protocol	From IP	From Port	To IP	To Port	Action	Comment	Log
1	All	0.0.0.0/0	any	0.0.0.0/0	any	Accept	default rule - please	No

Log entries for unknown connection attempts: No

**Outgoing**

Log ID: fw-vpn-v000\_000-out-Nº-3e8b12c4-3d40-1fd9-97e6-000cbe0220cf

No	Protocol	From IP	From Port	To IP	To Port	Action	Comment	Log
1	All	0.0.0.0/0	any	0.0.0.0/0	any	Accept	default rule - please	No

Log entries for unknown connection attempts: No

### Incoming (untrusted port), Outgoing (trusted port)

While the settings made in the *Network Security* menu only affect non-VPN connections (see above under “Network Security Menu (not for blade controller)” on page 162), the settings here only affect the VPN connection defined on these pages. This means that if multiple VPN connections are defined, you can restrict the outgoing or incoming access individually for each connection. You can log any attempts made to bypass these restrictions.

☒ The VPN firewall factory defaults are set to allow all connections via this VPN connection.

However, the extended firewall settings defined above (see “Network Security Menu (not for blade controller)”, “Network Security → Packet Filter”, “Advanced ” on page 169) apply independently for each individual VPN connection.

☒ If multiple firewall rules are set, they will be searched in the order in which they are listed (top-down) until a suitable rule is found. This rule is then applied. If there are other suitable rules further down the list, then these are ignored.

☒ In *Stealth* mode the actual IP address used by the client should be used in the firewall rules, or it should be left at 0.0.0.0/0. Only one client can be addressed through the tunnel.

☒ On the **Global** tab page, if the *Allow packet forwarding between VPN connections* switch is set to **Yes**, the rules under **Firewall Incoming** will be applied to the data packets coming into the mGuard, and the rules under **Firewall Outgoing** will be applied to the data packets going out. If the outgoing data packets are included in the same connection definition (in a defined VPN connection group), then the firewall rules for **Incoming** and **Outgoing** for the same connection definition are used. If a different VPN connection definition applies to the outgoing data packets, then the firewall rules for **Outgoing** for this other connection definition are used.

You have the following options:

### Protocol

**All** means: TCP, UDP, ICMP and other IP protocols.

### From / To IP

**0.0.0.0/0** means all IP addresses. To enter an address, use CIDR notation – see “CIDR (Classless Inter-Domain Routing)” on page 246.

Incoming:

From IP:           The IP address in the VPN tunnel

To IP:             The 1-to-1 NAT address or actual address

Outgoing:

From IP:           The 1-to-1 NAT address or actual address

To IP:             The IP address in the VPN tunnel

### From / To Port

(Only evaluated for TCP and UDP protocols)

**any** describes any selected port.

**startport:endport** (e.g. 110:120) defines a range of ports.

You can specify individual ports by giving either their port number or the corresponding service name: (e.g. 110 for pop3 or pop3 for 110).

### Action

**Accept** means that data packets may pass through.

**Reject** means that the data packets are rejected. The sender is informed that the data packets have been rejected. In *Stealth* mode, Reject has the same effect as Drop.

**Drop** means that data packets may not pass through. Data packets are discarded and the sender is not informed of their whereabouts.

### Comment

Freely selectable comment for this rule.

### Log

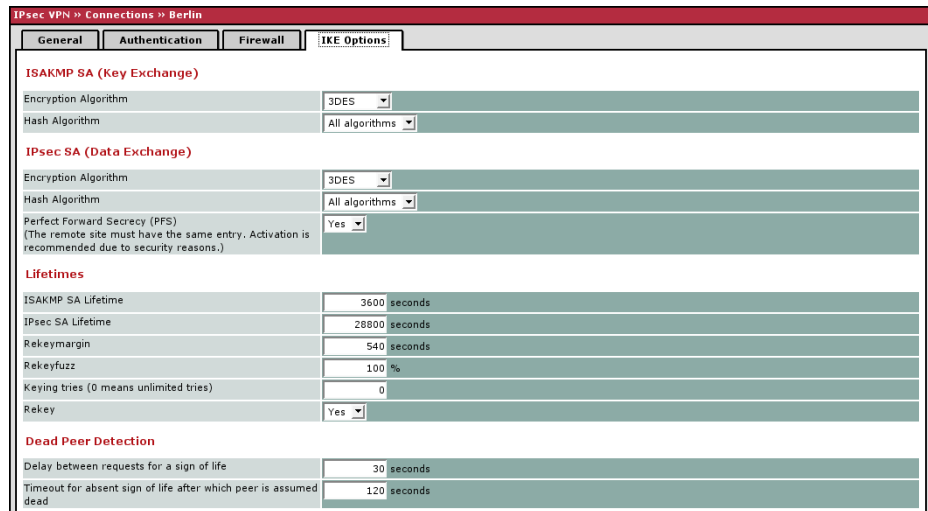
For each individual firewall rule you can specify whether the use of the rule

- should be logged (set *Log* to **Yes**) or
- should not be logged (set *Log* to **No** – factory default).

### Log entries for unknown connection attempts

When set to **Yes**, all attempts to establish a connection that are not covered by the rules defined above are logged.


## IKE Options



IPsec VPN » Connections » Berlin	
General Authentication Firewall IKE Options	
<b>ISAKMP SA (Key Exchange)</b>	
Encryption Algorithm	3DES
Hash Algorithm	All algorithms
<b>IPsec SA (Data Exchange)</b>	
Encryption Algorithm	3DES
Hash Algorithm	All algorithms
Perfect Forward Secrecy (PFS) (The remote site must have the same entry. Activation is recommended due to security reasons.)	Yes
<b>Lifetimes</b>	
ISAKMP SA Lifetime	3600 seconds
IPsec SA Lifetime	28800 seconds
Rekeymargin	540 seconds
Rekeyfuzz	100 %
Keying tries (0 means unlimited tries)	0
Rekey	Yes
<b>Dead Peer Detection</b>	
Delay between requests for a sign of life	30 seconds
Timeout for absent sign of life after which peer is assumed dead	120 seconds

### ISAKMP SA (Key Exchange)

#### Encryption Algorithm

 Decide on which encryption technique should be used with the remote peer administrator.

3DES-168 is the most commonly used algorithm and is therefore the default setting.

The following generally applies: The greater the number of bits used by an encryption algorithm (specified by the appended number) the more secure it is. The relatively new AES-256 protocol is therefore considered the most secure, but is not yet widely used.

The longer the key, the longer the time required by the encryption process. However, this is of no consequence for the mGuard as it uses a hardware-based encryption technique. This aspect may be of significance for the remote peer.

The algorithm designated as “Null” contains no encryption.

#### Hash Algorithm

Leave this setting as *All algorithms*. It then does not matter whether the remote peer uses MD5 or SHA-1.

### IPsec SA (Data Exchange)

In contrast to *ISAKMP SA (Key Exchange)* (see above), this setting determines the data exchange method. This may or may not be different from the Key Exchange method.

#### Encryption Algorithm


See above.

#### Hash Algorithm

See above.

#### Perfect Forward Secrecy (PFS)

This method is used to increase the security of the data transfer. In IPsec, the key used for the data exchange is changed at certain intervals. With PFS, a new random number is negotiated with the remote peer instead of deriving it from a previously agreed random number.

 Only set this to **Yes** if the remote peer supports PFS.

- ☞ Set *Perfect Forward Secrecy (PFS)* to **No** if the remote peer is an IPsec/L2TP client.

### **SA Lifetime**

The keys of an IPsec connection are renewed at certain intervals to increase the costs of an attack to the IPsec connection.

#### **ISAKMP SA Lifetime**

The lifetime of the ISAKMP SA keys in seconds. Factory default: 3600 seconds (1 hour). The permitted maximum is 86400 seconds (24 hours).

#### **IPsec SA Lifetime**

The lifetime of the IPsec SA keys in seconds.

Factory default: 28800 seconds (8 hours). The permitted maximum is 86400 seconds (24 hours).

#### **Rekeymargin**

Minimum time interval before the old key expires during which a new key should be created. Factory default: 540 seconds (9 minutes).

#### **Rekeyfuzz**

Maximum in percent by which *Rekeymargin* shall be randomly increased. This is used to delay key exchange on machines with many VPN connections. Factory default: 100%.

#### **Keying tries (0 means unlimited tries)**

Number of attempts to negotiate new keys with the remote peer.

The value 0 results in unlimited attempts for connections initiated by the mGuard, otherwise it results in 5.

#### **Rekey Yes / No**

When set to **Yes**, the mGuard will try to negotiate a new key when the old one expires.

### **Dead Peer Detection**

When the remote peer supports the Dead Peer Detection (DPD) protocol, both partners can detect whether the IPsec connection is still valid or must be restored.

#### **Delay between requests for a sign of life**

The time in seconds after which *DPD Keep Alive* queries are sent. These queries test whether the remote peer is still available.

Factory default: 30 seconds.

#### **Timeout for absent sign of life after which peer is assumed dead**

The time in seconds after which the remote peer is declared dead if *Keep Alive* queries are not answered.

Factory default: 120 seconds.

## **6.9.4 IPsec VPN → L2TP over IPsec**

Allows VPN connections using the IPsec/L2TP mGuard protocol.

In doing so, the L2TP protocol is driven using an IPsec transport connection in order to establish a tunnel connection with a Point-to-Point Protocol (PPP). Clients are automatically assigned IP addresses through PPP.

In order to use IPsec/L2TP, the L2TP server must be activated and one or more IPsec connections with the following characteristics must be defined:

- **Type:** Transport
- **Protocol:** UDP
- **Local port:** %any
- **Remote port:** %any
- **PFS:** No

(See also “→ Further settings can be made by clicking “More...”” on page 205 and “IKE Options” on page 215).

## L2TP Server

**IPsec VPN » L2TP over IPsec**

**L2TP Server**

**Settings**

Start L2TP Server for IPsec/L2TP?	Yes
Local IP for L2TP connections	10.106.106.1
Remote IP range start	10.106.106.2
Remote IP range end	10.106.106.254

*Please note: These rules won't apply to the Stealth mode.*

**Status**

Maximal number of tunnels	: 256
Tunnels in use	: 0
Maximal number of sessions per tunnel	: 16
Sessions in use	: 0
L2TP Daemon's Uptime	: 0 days and 00:00:03

### Settings

#### Start L2TP Server for IPsec/L2TP? Yes / No

If you want to enable IPsec/L2TP connections, set this option to **Yes**.

It is then possible to establish incoming L2TP connections over IPsec, which dynamically assign IP addresses to the clients within the VPN.

#### Local IP for L2TP connections

If set as shown in the screenshot above, the mGuard will inform the remote peer that its address is 10.106.106.1.

#### Remote IP range start / end

If set as shown in the screenshot above, the mGuard will assign the remote peer an IP address between 10.106.106.2 and 10.106.106.254.

### Status

Shows L2TP status information, when this connection type has been selected.

## 6.9.5 IPsec VPN → IPsec Status

IPsec VPN » IPsec Status					
Connection Name	Connection			ISAKMP State	IPsec State
Dublin (v001_001)	Gateway	192.168.66.1	%any		
<a href="#">Edit</a> <a href="#">Restart</a>	Traffic	host	host		
	ID				
London (v000_001)	Gateway	192.168.66.1	%any		
<a href="#">Edit</a> <a href="#">Restart</a>	Traffic	host	host		
	ID				

[Update](#)

Shows the status of IPsec connections.

The names of the VPN connections are listed on the left. On the right, you will find the current status of each connection.

## Buttons

### Update

Click on **Update** to update the displayed data.

### Restart

Click on **Restart** to terminate the connection and restart it again.

### Edit

Click on **Edit** to make changes to a configuration of the connection.

## Connection, ISAKMP Status, IPsec Status

### *GATEWAY*

Shows the IP addresses of the communicating VPN gateways

### *TRAFFIC*

Identifies the systems or networks which communicate via the VPN gateways.

### *ID*

Identifies the subject of an X.509 certificate.

### *ISAKMP State*

*ISAKMP State* (Internet security association and key management protocol) is given as “established” if both VPN gateways involved have established a channel for key exchange. In this case, they have contacted each other and all settings made on the configuration page up to and including “ISAKMP SA” were correct.

### *IPsec State*

*IPsec State* is given as “established” if IPsec encryption is activated during communication. In this case, the entries made under “IPsec SA” and “Tunnel Settings” were also correct.

In the event of problems, we recommend that you examine the VPN logs of the remote peer where the connection was setup. Detailed error messages are not returned to the initiating system for security reasons.

If the display shows:

*ISAKMP SA established, IPsec State: WAITING*

This indicates the following:

The authentication was successful, but the other parameters are incorrect. Do the connection types (Tunnel, Transport) match? If Tunnel has been selected, do the network address areas match on both sides?

If the display shows:

*IPsec State: IPsec SA established*

This indicates the following:

The VPN connection has been successfully set up and can be used. If this is not possible, there is a problem with the remote peer VPN gateway. In this case, disable and enable the connection again to re-establish the connection.

## 6.10 SEC-Stick Menu

The mGuard supports the use of an SEC-Stick. This provides access protection for IT systems. The SEC-Stick is a product of the team2work company: [www.team2work.de](http://www.team2work.de).

The SEC-Stick is a key. The user inserts it into the USB port of a computer with an Internet connection anywhere in the world. He can establish an encrypted connection to the mGuard then, which can be used to securely access services in his office network or his home. For example the Remote Desktop Protocol can be encapsulated within the encrypted and secure SEC-Stick connection to access the PC in the office or at home as if he were sitting directly in front of that PC.

This works because access to the business PC is protected by the mGuard and the mGuard can be configured for the SEC-Stick to permit access. The user of this remote computer, where the SEC-Stick is inserted, authenticates himself to the mGuard with the data stored on his SEC-Stick.

The SEC-Stick connects to the mGuard through SSH. Other channels can be embedded in this connection, e.g. TCP/IP connections.

### 6.10.1 Global

**SEC-Stick >> Global**

**Access**

**SEC-Stick Access**

Enable SEC-Stick service: No

Enable SEC-Stick remote access: No

Remote SEC-Stick TCP Port: 22002

**Allowed Networks**

N°	From IP	Interface	Action	Comment	Log
1	0.0.0.0/0	External	Accept		No

Log ID: fw-secstick-access-N°-00000000-0000-0000-0000-000000000000

These rules allow to enable SEC-Stick remote access.  
 Note: In Stealth mode incoming traffic on the given port is no longer forwarded to the client.  
 Note: In router mode with NAT or portforwarding the port set here has priority over portforwarding.  
 Note: The SEC-Stick access from the internal side and via dial-in is enabled by default and can be restricted by firewall rules.

## Access

### SEC-Stick Access

☒ A license is required for the SEC-Stick access function. It can only be used if the corresponding license has been purchased and installed.

#### Enable SEC-Stick service: Yes / No

By selecting **Yes**, you specify that the SEC-Stick being used at a remote location, or its owner, can login. In this case, the SEC-Stick remote access must also be enabled (next switch).

#### Enable SEC-Stick remote access: Yes / No

**Yes** enables the SEC-Stick remote access.

#### Remote SEC-Stick TCP Port

Default: 22002

If this port number is changed, the new port number only applies for access over the *External*, *External 2* or *VPN* interfaces. Port number 22002 still applies for internal access.

## Allowed Networks

Nº	From IP	Interface	Action	Comment	Log
1	0.0.0.0/0	External	Accept		No

These rules allow to enable SEC-Stick remote access.

Note: In Stealth mode incoming traffic on the given port is no longer forwarded to the client.

Note: In router mode with NAT or portforwarding the port set here has priority over portforwarding.

Note: The SEC-Stick access from the internal side and via dial-in is enabled by default and can be restricted by firewall rules.

Lists the firewall rules that have been set. They apply to SEC-Stick remote access.

If multiple firewall rules are set, they will be searched in the order in which they are listed (top-down) until a suitable rule is found. This rule is then applied. If there are other suitable rules further down the list, then these are ignored.

The rules specified here only become effective if **Enable SEC-Stick remote access** is set to **Yes**. *Internal* access is also possible when this option is set to *No*. A firewall rule that would refuse *Internal* access is therefore not effective in this case.

You can specify multiple rules. You have the following options:

### From IP

In this field you enter the address of the system or network where remote access is permitted or forbidden.

- IP address: **0.0.0.0/0** means all addresses. To enter an address, use CIDR notation – see “CIDR (Classless Inter-Domain Routing)” on page 246.

### Interface

**External / Internal / External 2 / VPN / Dial-in<sup>1</sup>**

Specifies which interface the rules apply to.

If no rules are set, the following default settings apply:

SEC-Stick remote access is permitted over *Internal*, *VPN* and *Dial-in*. Access over *External* and *External 2* is refused.

If required, you can specify the access possibilities.

### Caution:

If you want to refuse access over *Internal*, *VPN* or *Dial-in*, you must implement this explicitly through corresponding firewall rules, by specifying *Drop* as an action, for example.

### Action

Possible settings:

- Accept
- Reject
- Drop

**Accept** means that data packets may pass through.

**Reject** means that the data packets are rejected. The sender is informed that the data packets have been rejected. In *Stealth* mode, *Reject* has the same effect as *Drop* – see below.

**Drop** means that data packets may not pass through. The data packets are discarded and the sender is not informed of their whereabouts.

1. *External 2* and *Dial-in* only for devices with serial ports.  
See “Network → Interfaces” on page 105.

**Comment**

Freely selectable comment for this rule.

**Log**

For each individual firewall rule you can specify whether the use of the rule

- should be logged (set *Log* to **Yes**) or
- should not be logged (set *Log* to **No** – factory default)

## 6.10.2 Connections

Enabled	User Name	Name	Company
<input type="checkbox"/> No	drjansen	Dr. Norman Jansen	

### SEC-Stick Connections

#### SEC-Stick Connections

List of the defined SEC-Stick connections. Click on **Edit** to define a new connection or make changes to an existing connection.

**Enabled: Yes / No**

The **Enabled** switch must be set to **Yes** for a defined SEC-Stick connection to be used.

**User Name**

An SEC-Stick connection with a uniquely assigned user name must be defined for every owner of an SEC-Stick who has authorized access.

This user name is used to identify the defined connections.

**Name**

Name of the person.

**Company**

The name of the company.

The following page appears when you click on Edit:

The screenshot shows the 'SEC-Stick » Connections » drjansen' configuration page. It has two tabs: 'General' and 'SSH Port Forwarding'. The 'General' tab is active, showing fields for 'Enabled' (set to 'No'), 'User Name' (drjansen), 'A descriptive name of the user' (Dr. Norman Jansen), 'Company' (empty), and 'SSH public key (including ssh-dss or ssh-rsa)' (empty). The 'SSH Port Forwarding' tab shows a table with columns 'No', 'IP', and 'Port'. The first row has '1' in the 'No' column, '192.168.47.11' in the 'IP' column, and '3389' in the 'Port' column.

SEC-Stick connections		
<b>General</b>		
Enabled	No	
User Name	drjansen	
A descriptive name of the user	Dr. Norman Jansen	
Company		
SSH public key (including ssh-dss or ssh-rsa)		
<b>SSH Port Forwarding</b>		
No	IP	Port
1	192.168.47.11	3389

## General

### Enabled: Yes / No

As above

### User Name

As above

### A descriptive name of the user

Name of the person. (Repeated)

### Company

As above

### SSH public key (including ssh-dss or ssh-rsa)

Here you must enter the SSH public key belonging to the SEC-Stick in ASCII format. The secret equivalent is stored on the SEC-Stick.

## SSH Port Forwarding

List of the allowed access and SSH port forwarding relating to the SEC-Stick of the corresponding user.

### IP

IP address of the computer to which the access is allowed.

### Port

Port number to be used when accessing the computer.

☒ Not all the functions of the SEC-Stick can be configured using the web interface of the mGuard.

## 6.11 QoS Menu

QoS (Quality of Service) defines the quality of individual transfer channels in IP networks. This relates to the allocation of certain resources to certain services or communication types so that they work correctly. For example, the necessary bandwidth must be provided for the transfer of audio or video data in real time in order to reach a satisfactory communication level. At the same time, a slower data transfer by FTP or email does not threaten the overall success of the transfer (file or email transfer).

### 6.11.1 Ingress Filter

An Ingress Filter prevents the processing of certain data packages by filtering and dropping them before they enter the processing mechanism. The mGuard can use an Ingress Filter to avoid processing data packets that are not needed in the network. This results a quicker processing of remaining (required) data packages. Using suitable filter rules, administrative access to the mGuard can be ensured with high probability.

Package processing on the mGuard is generally defined by the handling of individual data packages so that the processing performance depends on the number of packets and not on bandwidth.

Filtering is only made according to characteristics that are present in each data packet: The sender's IP address in the header, ethernet protocol, IP protocol, TOS/DSCP value and/or the VLAN ID (if VLAN has been configured). As the list of filter rules must be applied to each individual data packet, it should be kept as short as possible. Otherwise, the time spent on filtering could be longer than the time saved by setting the filter itself.

Please note that not all filter criteria can be combined. For example, it does not make sense to enter an additional IP protocol in the same set of rules as the ARP ethernet protocol. This also applies to the entry of a sender or recipient IP address under the hexadecimal IPX ethernet protocol.

#### Internal / External

QoS » Ingress Filters											
Internal External											
<b>Enabling</b>											
Enable Ingress QoS										No	
Measurement Unit										Packet/s	
<b>Filters</b>											
	No	Use VLAN	VLAN ID	Ethernet Protocol	IP Protocol	From IP	To IP	Current TOS/DSCP	Guaranteed	Upper Limit	Comment
	<input checked="" type="checkbox"/>	No		ARP	All	0.0.0.0/0	0.0.0.0/0	All	100	unlimited	

Internal: Setting of Ingress Filters on the LAN interface

QoS » Ingress Filters											
Internal External											
<b>Enabling</b>											
Enable Ingress QoS										No	
Measurement Unit										Packet/s	
<b>Filters</b>											
	No	Use VLAN	VLAN ID	Ethernet Protocol	IP Protocol	From IP	To IP	Current TOS/DSCP	Guaranteed	Upper Limit	Comment
	<input checked="" type="checkbox"/>	No		ARP	All	0.0.0.0/0	0.0.0.0/0	All	100	unlimited	

External: Setting of Ingress Filters on the WAN interface

## Enabling

### Enable Ingress QoS: Yes / No

**No** (standard): Feature is disabled. If filter rules are defined, then they are ignored.

**Yes:** Feature is enabled. Data packets will only be transferred to the mGuard for further processing when they conform to the following filter rules.

Filters can be set for the LAN port (**Internal** tab) and WAN port (**External** tab).

### Units: kbit/s / packets/s

Defines in which format the values below under **Guaranteed** and **Upper Limit** are defined.

## Filter

### Use VLAN: Yes / No

If VLAN is configured, then the VLAN ID can be entered to allow the affected data packets to pass through. The option must be set to **Yes**.

### VLAN ID

Defines that the VLAN data packets that have this ID may pass through. (The **Use VLAN** option must be set to **Yes**.)

### Ethernet Protocol

Defines that only data packets from the given ethernet protocol may pass. Possible entries: **ARP**, **IPv4**, **%any**. Other entries must be given in hexadecimal form (up to 4 figures).

(The entry here is the ID of the affected protocol that can be found in the ethernet header. This can be found in the publication of the affected standard.)

### IP Protocol: All / TCP / UDP / ICMP /ESP

Defines that only data packets from the selected IP protocol may pass. When **All** is selected, no filtering is made according to the IP protocol.

### From IP

Defines that only data packets from the given IP address may pass.

**0.0.0.0/0** stands for all addresses. This means that no filtering is made according to the IP address of the sender. To enter an address, use **CIDR** notation – see “CIDR (Classless Inter-Domain Routing)” on page 246.

### To IP

Defines that only data packets that should be forwarded to the given IP address may pass through.

Entries correspond to *From IP*, as detailed above.

**0.0.0.0/0** stands for all addresses. This means that no filtering is made according to the IP address of the sender.

### Current TOS/DSCP

Each data packet contains a TOS or DSCP field (TOS stands for Type Of Service, DSCP for Differentiated Services Code Point). The traffic type to which the data packet belongs is specified here. An IP telephone, for example, will therefore write something different into this field than an FTP program.

When a value is selected here, then only data packets with this value in the TOS or DSCP field may pass through. When **All** is selected, no filtering is made according to the TOS/DSCP value.

### **Guaranteed**

The entered number defines how many data packets or kbit/s can pass through at all times (according to the set **units** – see above). This applies to the data flow that conforms to the set of rules criteria listed on the left (i.e. that may pass through). The mGuard may drop the excess number of data packets during capacity bottlenecks if this data flow delivers more data packets per second.

### **Upper Limit (kbit/s)**

The entered number defines the maximum number of data packets or kbit/s that can pass through (according to the set **units** – see above). This applies to the data flow that conforms to the set of rules criteria listed on the left (i.e. that may pass through). The mGuard will drop the excess number of data packets if this data flow delivers more data packets per second.

### **Comment**

Optional: Text comment.

### 6.11.2 Egress Queues

The services are allocated according to defined priorities. During connection bottlenecks, the outgoing data packets are put into egress queues (i.e. queues for waiting packets), and are then processed according to their priority. Ideally, the allocation of priority levels and bandwidths should result in a sufficient bandwidth level being available for the complete transfer of data packets in real-time, whilst other packets (e.g. FTP downloads) are set to wait in critical cases.

The main function of Egress QoS is the optimal utilization of the available bandwidth on a connection. In certain cases, a limitation of the packet rate can be useful (e.g. to protect a slow computer from overloading in the protected network).

The *Egress Queues* feature can be used for all interfaces and for VPN connections.

#### Internal / External / External 2 / Dial-in

N°	Name	Guaranteed	Upper Limit	Priority	Comment
1	Urgent	10	unlimited	High	
2	Important	10	unlimited	Medium	
3	Default	10	unlimited	Medium	
4	Low Priority	10	unlimited	Low	

Internal: Setting of Egress Queues on the LAN interface

N°	Name	Guaranteed	Upper Limit	Priority	Comment
1	Urgent	10	unlimited	High	
2	Important	10	unlimited	Medium	
3	Default	10	unlimited	Medium	
4	Low Priority	10	unlimited	Low	

External: Setting of Egress Queues on the external WAN interface

N°	Name	Guaranteed	Upper Limit	Priority	Comment
1	Urgent	10	unlimited	High	
2	Important	10	unlimited	Medium	
3	Default	10	unlimited	Medium	
4	Low Priority	10	unlimited	Low	

External 2: Setting of Egress Queues on the secondary external interface

N°	Name	Guaranteed	Upper Limit	Priority	Comment
1	Urgent	10	unlimited	High	
2	Important	10	unlimited	Medium	
3	Default	10	unlimited	Medium	
4	Low Priority	10	unlimited	Low	

Dial-in: Setting of Egress Queues for packets for PPP dial connection (dial-in)

### 6.11.3 Egress Queues (VPN)

VPN via Internal /  
VPN via External /  
VPN via External 2 /  
VPN via Dial-in

**VPN via Internal** | VPN via External | VPN via External 2 | VPN via Dial-in

**Enabling**

Enable Egress QoS

**Total Bandwidth/Rate**

Bandwidth/Rate Limit  kbit/s

**Queues**

#	Name	Guaranteed	Upper Limit	Priority	Comment
1	Urgent	10	unlimited	High	
2	Important	10	unlimited	Medium	
3	Default	10	unlimited	Medium	
4	Low Priority	10	unlimited	Low	

VPN via Internal: Setting of Egress Queues

**VPN via Internal** | **VPN via External** | VPN via External 2 | VPN via Dial-in

**Enabling**

Enable Egress QoS

**Total Bandwidth/Rate**

Bandwidth/Rate Limit  kbit/s

**Queues**

#	Name	Guaranteed	Upper Limit	Priority	Comment
1	Urgent	10	unlimited	High	
2	Important	10	unlimited	Medium	
3	Default	10	unlimited	Medium	
4	Low Priority	10	unlimited	Low	

VPN via External: Setting of Egress Queues

**VPN via Internal** | **VPN via External** | **VPN via External 2** | VPN via Dial-in

**Enabling**

Enable Egress QoS

**Total Bandwidth/Rate**

Bandwidth/Rate Limit  kbit/s

**Queues**

#	Name	Guaranteed	Upper Limit	Priority	Comment
1	Urgent	10	unlimited	High	
2	Important	10	unlimited	Medium	
3	Default	10	unlimited	Medium	
4	Low Priority	10	unlimited	Low	

VPN via External 2: Setting of Egress Queues

**VPN via Internal** | **VPN via External** | **VPN via External 2** | **VPN via Dial-in**

**Enabling**

Enable Egress QoS

**Total Bandwidth/Rate**

Bandwidth/Rate Limit  kbit/s

**Queues**

#	Name	Guaranteed	Upper Limit	Priority	Comment
1	Urgent	10	unlimited	High	
2	Important	10	unlimited	Medium	
3	Default	10	unlimited	Medium	
4	Low Priority	10	unlimited	Low	

VPN via Dial-in: Setting of Egress Queues

All the tab pages listed above for *Egress Queues* for the *Internal*, *External*, *External 2*, *Dial-in* interfaces, and for VPN connections made over these interfaces, provide the same setting possibilities.

In all cases the settings relate to the data that is sent externally to the network from the respective mGuard interface.

**Enabling****Enable Egress QoS: Yes / No**

**No** (standard): Feature is disabled.

**Yes:** Feature is enabled. This is recommended when the interface is connected to a network with a small bandwidth. This allows the bandwidth allocation to be influenced in favor of especially important data.

**Total Bandwidth****Maximum bandwidth/rate ..... kBit/s / packets/s**

Maximum available bandwidth – measured in kbit/s or packets/s.

In order for an optimal prioritization process, the total bandwidth entered here should be slightly lower than the actual amount. This prevents an overrun in the transferring device buffer, which would create adverse effects.

**Queues****Name**

You can apply the preset name for the Egress Queues or select another one. The name does not define data priority.

**Guaranteed**

Bandwidth that should be available for the relevant queue. Use the same units as defined above under **Maximum bandwidth/rate (kbit/s OR packets/s)** but do not enter the units of measurement explicitly.

The total of all guaranteed bandwidths must be smaller or equal to the total bandwidth.

**Upper Limit (kbit/s)**

Maximum permitted bandwidth available for the relevant queue. Use the same units as defined above under **Maximum bandwidth/rate (kbit/s OR packets/s)** but do not enter the units of measurement explicitly.

This value must be the same as or larger than the guaranteed bandwidth.

You can also enter the **unlimited** setting, which means no further restriction.

**Priority: Low / Medium / High**

Defines with which priority the affected queue should be processed, providing the total available bandwidth is not exhausted.

**Comment**

Optional: Text comment.

## 6.11.4 Egress Rules

This page defines which data is assigned to the defined Egress Queues (see above).

Rules can be defined separately for all interfaces and also for VPN connections.

### Internal / External / External 2 / Dial-in

**QoS -> Egress Rules**

Internal External External 2 Dial-in

**Default**

Default Queue: Default

**Rules**

No	Protocol	From IP	From Port	To IP	To Port	Current TOS/DSCP	New TOS/DSCP	Queue Name	Comment
1	All	0.0.0.0/0	any	0.0.0.0/0	any	TOS: Minimize Delay	Unchanged	Urgent	
2	All	0.0.0.0/0	any	0.0.0.0/0	any	TOS: Maximize Reliability	Unchanged	Important	
3	All	0.0.0.0/0	any	0.0.0.0/0	any	TOS: Minimize Cost	Unchanged	Low Priority	

Internal: Setting of Egress Queue rules

**QoS -> Egress Rules**

Internal External External 2 Dial-in

**Default**

Default Queue: Default

**Rules**

No	Protocol	From IP	From Port	To IP	To Port	Current TOS/DSCP	New TOS/DSCP	Queue Name	Comment
1	All	0.0.0.0/0	any	0.0.0.0/0	any	TOS: Minimize Delay	Unchanged	Urgent	
2	All	0.0.0.0/0	any	0.0.0.0/0	any	TOS: Maximize Reliability	Unchanged	Important	
3	All	0.0.0.0/0	any	0.0.0.0/0	any	TOS: Minimize Cost	Unchanged	Low Priority	

External: Setting of Egress Queue rules

**QoS -> Egress Rules**

Internal External External 2 Dial-in

**Default**

Default Queue: Default

**Rules**

No	Protocol	From IP	From Port	To IP	To Port	Current TOS/DSCP	New TOS/DSCP	Queue Name	Comment
1	All	0.0.0.0/0	any	0.0.0.0/0	any	TOS: Minimize Delay	Unchanged	Urgent	
2	All	0.0.0.0/0	any	0.0.0.0/0	any	TOS: Maximize Reliability	Unchanged	Important	
3	All	0.0.0.0/0	any	0.0.0.0/0	any	TOS: Minimize Cost	Unchanged	Low Priority	

External 2: Setting of Egress Queue rules

**QoS -> Egress Rules**

Internal External External 2 Dial-in

**Default**

Default Queue: Default

**Rules**

No	Protocol	From IP	From Port	To IP	To Port	Current TOS/DSCP	New TOS/DSCP	Queue Name	Comment
1	All	0.0.0.0/0	any	0.0.0.0/0	any	TOS: Minimize Delay	Unchanged	Urgent	
2	All	0.0.0.0/0	any	0.0.0.0/0	any	TOS: Maximize Reliability	Unchanged	Important	
3	All	0.0.0.0/0	any	0.0.0.0/0	any	TOS: Minimize Cost	Unchanged	Low Priority	

Dial-in: Setting of Egress Queue rules

### 6.11.5 Egress Rules (VPN)

VPN via Internal /  
VPN via External /  
VPN via External 2 /  
VPN via Dial-in

The screenshot shows the 'QoS Egress Rules (VPN)' configuration page with the 'VPN via Internal' tab selected. The 'Default Queue' is set to 'Default'. The 'Rules' table contains three entries:

#	Protocol	From IP	From Port	To IP	To Port	Current TOS/DSCP	New TOS/DSCP	Queue Name	Comment
1	All	0.0.0.0/0		0.0.0.0/0		TOS: Minimize Delay	Unchanged	Urgent	
2	All	0.0.0.0/0		0.0.0.0/0		TOS: Maximize Reliability	Unchanged	Important	
3	All	0.0.0.0/0		0.0.0.0/0		TOS: Minimize Cost	Unchanged	Low Priority	

VPN via Internal: Setting of Egress Queue rules

The screenshot shows the 'QoS Egress Rules (VPN)' configuration page with the 'VPN via External' tab selected. The 'Default Queue' is set to 'Default'. The 'Rules' table contains three entries:

#	Protocol	From IP	From Port	To IP	To Port	Current TOS/DSCP	New TOS/DSCP	Queue Name	Comment
1	All	0.0.0.0/0		0.0.0.0/0		TOS: Minimize Delay	Unchanged	Urgent	
2	All	0.0.0.0/0		0.0.0.0/0		TOS: Maximize Reliability	Unchanged	Important	
3	All	0.0.0.0/0		0.0.0.0/0		TOS: Minimize Cost	Unchanged	Low Priority	

VPN via External: Setting of Egress Queue rules

The screenshot shows the 'QoS Egress Rules (VPN)' configuration page with the 'VPN via External 2' tab selected. The 'Default Queue' is set to 'Default'. The 'Rules' table contains three entries:

#	Protocol	From IP	From Port	To IP	To Port	Current TOS/DSCP	New TOS/DSCP	Queue Name	Comment
1	All	0.0.0.0/0		0.0.0.0/0		TOS: Minimize Delay	Unchanged	Urgent	
2	All	0.0.0.0/0		0.0.0.0/0		TOS: Maximize Reliability	Unchanged	Important	
3	All	0.0.0.0/0		0.0.0.0/0		TOS: Minimize Cost	Unchanged	Low Priority	

VPN via External 2: Setting of Egress Queue rules

The screenshot shows the 'QoS Egress Rules (VPN)' configuration page with the 'VPN via Dial-in' tab selected. The 'Default Queue' is set to 'Default'. The 'Rules' table contains three entries:

#	Protocol	From IP	From Port	To IP	To Port	Current TOS/DSCP	New TOS/DSCP	Queue Name	Comment
1	All	0.0.0.0/0		0.0.0.0/0		TOS: Minimize Delay	Unchanged	Urgent	
2	All	0.0.0.0/0		0.0.0.0/0		TOS: Maximize Reliability	Unchanged	Important	
3	All	0.0.0.0/0		0.0.0.0/0		TOS: Minimize Cost	Unchanged	Low Priority	

VPN via Dial-in: Setting of Egress Queue rules

All the tab pages listed above for *Egress Queues* for the *Internal*, *External*, *External 2*, *Dial-in* interfaces, and for VPN connections made over these interfaces, provide the same setting possibilities.

In all cases the settings relate to the data that is sent externally to the network from the respective mGuard interface.

## Default

### Default Queue: Names of the Egress Queues (user-defined)

The names of queues are displayed as listed or defined under *Egress Queues* on the *Internal / External / VPN via External* tabs. The following names are defined as standard: Default / Urgent / Important / Low Priority

Traffic that is not allocated to an Egress Queue under *Rules* remains in the *Default Queue*. You can specify which Egress Queue is used as the *Default Queue* in this selection list.

## Rules

The allocation of certain data traffic to an Egress Queue is made using its source and destination, given as IP address and port respectively.

Example:

You have defined a queue with guaranteed bandwidth and priority for transferred audio data under QoS → Egress Queues (see “Egress Queues” on page 227) under the name *Urgent*. You specify here the rules for how the audio data is defined, and that this data belongs in the *Urgent* queue.

### Protocol: All / TCP / UDP / ICMP /ESP

Protocols relating to the allocation.

### From IP

IP address of the network or device where the data originates from.

**0.0.0.0/0** means all IP addresses. To enter an address, use CIDR notation – see “CIDR (Classless Inter-Domain Routing)” on page 246.

Allocate the traffic from this source to a queue towards the back of this row by entering the *Queue name*.

### From Port

Port used at the source where the data originates from (only evaluated for TCP and UDP protocols).

**any** describes any selected port.

**startport:endport** (e.g. 110:120) defines a range of ports.

You can specify individual ports by giving either their port number or the corresponding service name: (e.g. 110 for pop3 or pop3 for 110).

### To IP

IP address of the network or device where the data is sent to. Entries correspond to *From IP*, as detailed above.

### To Port

Port used at the source where the data is sent to. Entries correspond to *From Port*, as detailed above.

### Current TOS/DSCP

Each data packet contains a TOS or DSCP field (TOS stands for Type Of Service, DSCP for Differentiated Services Code Point). The traffic type to which the data packet belongs is specified here. For example, an IP telephone writes outgoing data packets differently into this field than a FTP program that loads the data packages to a server.

When you select a value here, only the data packets that have this TOS or DSCP value in the corresponding fields are chosen. This sets a different value according to the entry in the **New TOS/DSCP** field.

**New TOS/DSCP**

If you want to change the TOS/DSCP values of the data packets that are selected using the defined rules, then enter what should be written in the TOS or DSCP field here.

You can also accept the filled TOS field as the only allocation criteria. This occurs when the source and destination IP addresses and ports are freely defined and the TOS field has a specific value.

Further details concerning the **Current TOS/DSCP** and **New TOS/DSCP** can be found in the following RFC documentation:

- RFC3260 “New Terminology and Clarifications for Diffserv”
- RFC3168 “The Addition of Explicit Congestion Notification (ECN) to IP”
- RFC2474 “Definition of the Differentiated Services Field (DS Field)”
- RFC1349 “Type of Service in the Internet Protocol Suite”

**Queue Name**

Name of the Egress Queue where the traffic is assigned.

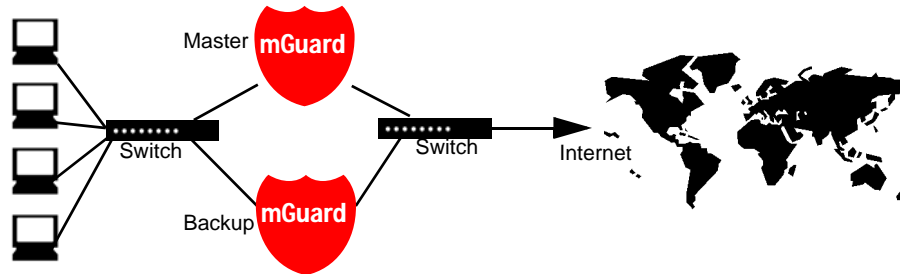
**Comment**

Optional: Text comment.

## 6.12 Redundancy Menu

### 6.12.1 Firewall Redundancy

Using redundancy, it is possible to combine two mGuards in a single virtual router.



In the event of an error, the second mGuard (backup) takes over the function of the first mGuard (master).

Additionally, the state of the stateful firewall is synchronized between both mGuards so that current connections are not interrupted during a changeover.

- ☒ Requirement: Both mGuards must be configured accordingly. The firewall configuration should be identical to avoid problems after a switch-over.
- ☒ Redundancy is supported in the following network modes: *Router mode*, *static Stealth mode* with Management IP and in *Stealth mode (several clients)*.
- ☒ Redundancy is not supported if the *External 2<sup>1</sup>* interface is activated.
- ☒ If the two mGuards are operated in the *Stealth Mode* network mode *statically* with Management IP or in *Stealth Mode (multiple clients)*, DAD ARP requests are sent on the internal interface when one of the mGuard takes over the function of the other (see RFC2131, section 4.4.1).
- ☒ Both mGuards may not be used as a VPN gateway when redundancy is activated.
- ☒ When redundancy is activated, the user firewall logins cannot be synchronized between the mGuards. The mGuard does not provide a user interface at the virtual IP address. Therefore it is not possible to login there as a user of the user firewall.
- ☒ Devices connected to the mGuard LAN port must be configured to use the mGuard's internal virtual IP address (see below) as the standard gateway.

The following features can be used when redundancy is activated – see “Network Security Menu (not for blade controller)”:

- Incoming/outgoing firewall rules
- NAT (IP Masquerading, i.e. outgoing network traffic is rewritten to the external virtual IP)
- 1:1 NAT
- Port forwarding (the external virtual IP must be configured as *Incoming on IP*)
- MAC Filtering

---

1. *External 2* only for devices with serial ports.  
See “Network → Interfaces” on page 105.

Redundancy » Firewall Redundancy	
Redundancy	ICMP Checks
<b>General</b>	
Redundancy State	Disabled
Enable Redundancy	No
Redundancy Start State	Master
Priority	100
Authentication passphrase	passwd
Stealth Mode: Virtual Router ID	51
Router Mode: External Virtual Router ID	
Stealth Mode: Management IP of the 2nd device	10.0.0.1
Router Mode: External IP of the 2nd device	
<b>Router Mode</b>	
Internal Virtual Router ID	52
Internal IP of the 2nd device	192.168.1.1
External virtual IP	10.0.0.100
Internal virtual IP	192.168.1.100

## Redundancy

### General

#### Redundancy State

Shows the current state.

#### Enable Redundancy: Yes / No

Enable/disable the redundancy feature.

#### Redundancy Start State

State of the mGuard during activation of redundancy (*Master* or *Backup*).

#### Priority

Defines which mGuard operates as the master.

If priorities are set differently, the mGuard with the higher priority operates as the master as long as it does not fail.

If both mGuards have the same priority and the backup becomes the master in case of a failure, it continues to work as the master even when the other mGuard becomes available again.

Values between 1 and 254 are possible.

#### Authentication passphrase

This password protects against wrong configuration among different virtual routers.

The password must be the same on both mGuards. It is transmitted in clear text and should not be identical with other security-relevant passwords.

#### Stealth Mode: Virtual Router ID

#### Router Mode: External Virtual Router ID

An ID between 1 and 255 which must be the same on both mGuards and identifies the virtual router.

#### Stealth mode: Management IP of the 2nd device

#### Router Mode: External IP of the 2nd device

The management IP of the second mGuard (in Stealth mode), or the external IP of the second mGuard (in Router mode).

## Router Mode

The following values must be set if the mGuards are operated in router mode.

### Internal Virtual Router ID

An ID between 1 and 255 which must be the same on both mGuards.  
This ID identifies the virtual router on the LAN port.

### Internal IP of the 2nd device

The internal IP of the second mGuard LAN port.

### External virtual IP

Virtual IP address where the data traffic runs through the mGuard.  
For example, used by NAT as external IP. Can be freely defined, providing it is actually contained in the externally configured network and the IP address is not in use there.

### Internal virtual IP

Virtual IP address where the data traffic runs through the mGuard.  
For example, these must be set as the default gateway for clients on the LAN port of the mGuard connected to the network.

Can be freely defined, providing it is actually contained in the internally configured network and the IP address is not in use there.

## ICMP Checks

The screenshot shows the 'Redundancy >> Firewall Redundancy' configuration page. It has two tabs: 'Redundancy' and 'ICMP Checks', with the latter being selected. The 'ICMP Checks' section contains the following settings:

ICMP Checks	
Enable ICMP checks	No
Hosts to check via ICMP in the external network	<div>IP: 10.0.0.30</div>
Hosts to check via ICMP in the internal network	<div>IP: 192.168.1.30</div>

ICMP checks provide an additional way of monitoring the network connections between mGuards working as a virtual router.

If one of the two direct ethernet connections that exist between the LAN ports of the two mGuards (left of both mGuards in the drawing on Page 234) and between the WAN ports (right of both mGuards in the drawing) fails, the backup becomes the master. However, the Virtual Router Redundancy Protocol (VRRP) used by the Guard cannot inform the master of this while it is still operating. In such cases the two masters would then be in conflict over the existing network connection.

With ICMP checks (ICMP ping), the master can check the connection to the backup and deactivate itself if needed.

**Enable ICMP Checks: Yes / No**

When **Yes** is selected, the connection to the backup is monitored using the ICMP protocol.

If the backup mGuard is not accessible, the master attempts to access the hosts entered under *Hosts to check via ICMP in the external/internal network* successively.

If these are also not accessible, the master mGuard deactivates itself.

**Hosts to check via ICMP in the external network****Hosts to check via ICMP in the internal network**

Enter the respective IP address here.

The hosts must answer ICMP echo requests.

**6.12.2 Ring / Network Coupling****Ring / Network Coupling**

Redundancy >> Ring/Network Coupling	
Ring/Network Coupling	
Settings	
Enable Ring/Network Coupling/Dual Homing	No
Redundancy Port	Internal

**Settings****Enable Ring/Network Coupling/Dual Homing: Yes / No**

When activated, the status of one ethernet port is transferred in Stealth mode to the next port. This means that interruptions in the network can be traced more easily.

**Redundancy Port: Internal / External**

Internal: The WAN port is activated/deactivated accordingly when the connection on the LAN port is connected/disconnected.

External: The LAN port is activated/deactivated accordingly when the connection on the WAN port is connected/disconnected.

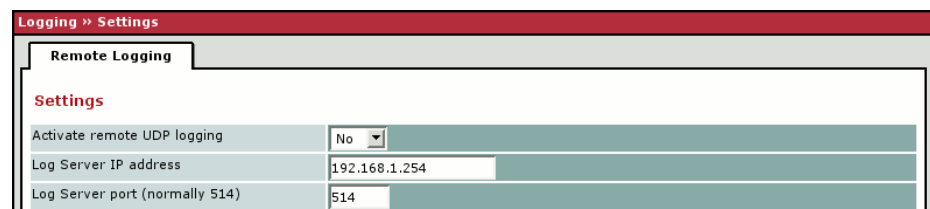
## 6.13 Logging Menu

Logging is the recording of event messages (e.g. concerning settings that have been made, firewall rules taking effect, errors etc.).

Log entries are recorded in different categories and can be displayed according to these categories – see “Logging → Browse local logs” on page 239.

### 6.13.1 Logging → Settings

#### Remote Logging



Logging » Settings	
Remote Logging	
Settings	
Activate remote UDP logging	No
Log Server IP address	192.168.1.254
Log Server port (normally 514)	514

All log entries are recorded by default in the mGuard's temporary memory (RAM). Once the memory for log entries has been filled, the oldest log entries are overwritten. Furthermore, all log entries are deleted when the mGuard is switched off.

To prevent this, the log entries can be transferred to an external system. This is particularly useful if you wish to have centralized administration of the logs.


#### Settings

##### Activate remote UDP logging: Yes / No

If all log entries should be sent to an external log server (specified below), set this option to **Yes**.

##### Log Server IP address

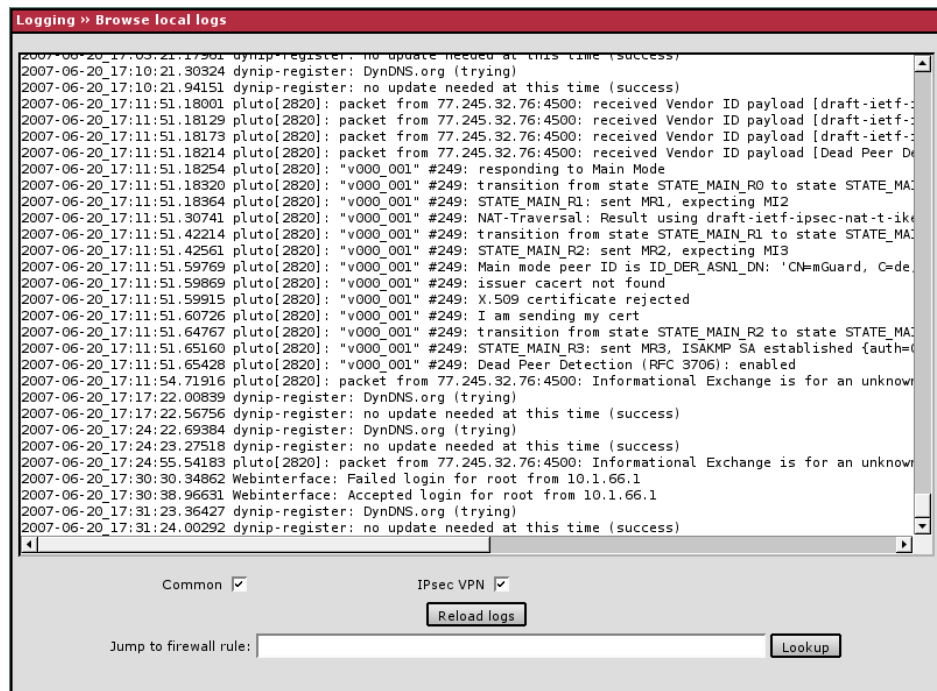
Enter the IP address of the log server where the log entries should be sent via UDP.

 This entry must be an IP address – not a hostname! This function does not support hostnames, as it would otherwise not be possible to log the loss of a DNS server.

##### Log Server port (normally 514)

Enter the port of the log server where the log entries should be sent via UDP. Standard: 514

### 6.13.2 Logging → Browse local logs



The corresponding checkboxes for filtering entries according to category are displayed below the log entries depending on which mGuard functions were active.

To display one or more categories, enable the checkboxes for the desired categories and click the **Reload logs** button.

#### Log entry categories

##### Common

Log entries which are not assigned to other categories.

##### Network Security

Logged events are shown here when the logging of firewall events was selected during the definition of firewall rules (Log = Yes).

#### Log ID and number for tracing errors

Log entries that refer to the firewall rules listed below have a log ID and number. Using this log ID and number, it is possible to trace the firewall rule that the corresponding log entry refers to and that led to the event in question.

##### Firewall rules and their log ID

- Packet filters:  
Network Security → Packet Filters → Incoming Rules / Outgoing Rules menu  
Log ID: **fw-incoming** or **fw-outgoing**
- Firewall rules for VPN connections:  
IPsec VPN → Connections → Firewall Incoming / Outgoing menu  
Log ID: **vpn-fw-in** or **vpn-fw-out**
- Firewall rules for web access through mGuard via HTTPS:  
Management → Web Settings → Access menu  
Log ID: **fw-https-access**

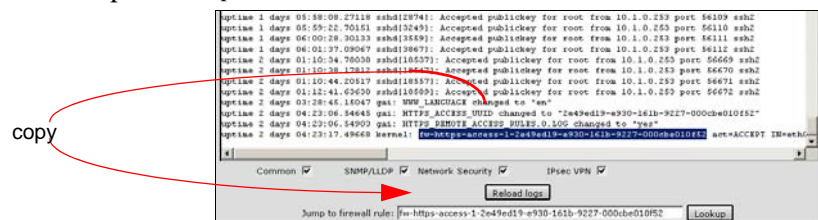
- Firewall rules for web access through mGuard via SNMP:  
Management → SNMP → Query menu  
Log ID: **fw-snmpp-access**
- Firewall rules for SSH remote access to the mGuard:  
Management → System settings → Shell Access menu  
Log ID: **fw-ssh-access**
- Firewall rules for the user firewall:  
Network Security → User Firewall → Firewall Rules menu  
Log ID: **ufw-**
- Rules for NAT, port forwarding:  
Network Security → NAT → Port Forwarding menu  
Log ID: **fw-portforwarding**
- Firewall rules for serial port:  
Network → Interfaces → Serial Port  
Incoming Rules  
Log ID: **fw-serial-incoming**  
Outgoing Rules  
Log ID: **fw-serial-outgoing**

### Searching for firewall rules on the basis of a network security log

If the **Network Security** checkbox is enabled so that the relevant log entries are displayed, the **Jump to firewall rule** search field is displayed under the *Reload Logs* button.

Proceed as follows if you want to trace the firewall rule referenced by a log entry in the *network security* category that resulted in the relevant event:

1. Mark the section that contains the log ID and number in the relevant log entry, for example: fw-https-access-1-1ec2c133-dca1-1231-bfa5-000cbe01010a



2. Copy this section into the **Jump to firewall rule** field via the clipboard.
3. Click on the **Lookup** button.

Result:

The configuration page containing the firewall rule that the log entry refers to is displayed.

## Blade

In addition to error messages, the following messages are output on the blade controller:

The areas enclosed by < and > are replaced by the respective data in the log entries.

### General messages:

```
blade daemon "<version>" starting ...
Blade[<bladenr>] online
Blade[<bladenr>] is mute
Blade[<bladenr>] not running
Reading timestamp from blade[<bladenr>]
```

### When activating a configuration profile on a blade:

```
Push configuration to blade[<bladenr>]
reconfiguration of blade[<bladenr>] returned <returncode>
blade[<bladenr>] # <text>
```

### When retrieving a configuration profile from a blade:

```
Pull configuration from blade[<bladenr>]
Pull configuration from blade[<bladenr>] returned <returncode>
```

## Anti-virus

The anti-virus log contains the following messages from the virus filter:

- Any detected viruses together with the relevant details (virus name, file name, plus (in the case of an email): sender, date and subject).
- Warnings sent when pass-through mode is activated automatically due to excessive size and unscanned file.
- Startup and shutdown of the virus filter programs.
- Error messages from the anti-virus filter.

### Error Messages:

#### Virus Detection

A virus has been detected. The error message includes the name of the virus, the sender of the email, the date sent, the name of the infected file or the name of the compressed archive file and the infected portion of this archive.

An example of a virus message:

```
mGuard detected a virus. The mail could not be delivered.
found Virus Email-Worm.Win32.NetSky.q /[From
sick@example.com][Date Fri, 13 Aug 2004 11:33:53++0200]/
about_you.zip/document.txt.exe
[000012a7.000000077.000000000]
Message Details:
From: sick@example.com
Subject: Private document
Date: Fri, 13 Aug 2004 11:33:53 +0200
```

### **Exceeded maximum filesize**

The maximum filesize set for this protocol was exceeded.

To transfer the file anyway, you can deactivate the virus filter either globally or for the corresponding server over the course of the download. Alternatively, you can set the “Action for ...exceeding the maximum message size” parameter to “Let the message/data pass unscanned” under the *Web Security* or *Email Security* menu.

☒ In both cases, the transferred files are not scanned for viruses!

### **Temporary Virus Scanner Failure**

A temporary error occurred while trying to scan a file. Repeating the transfer later or updating the virus signature file may solve this problem.

Possible causes:

- The scan engine cannot process the file
- The mGuard does not have enough available memory to decompress the file
- Internal error in the scan engine

### **Exceptional Virus Scanner Failure**

A problem has occurred during communication with the scan engine.

Possible causes:

- Failed signature update due to wrong update server entries (see Management -> Update menu)
- Invalid virus filter license
- Damaged or faulty update of the virus signature file

### **Update running**

There is currently no anti-virus filter signature installed, and the download of the virus signatures has been started. You can follow the progress of the download in the anti-virus update log (Logging -> Browse local logs -> Anti-virus update).

## **DHCP Server/Relay**

Messages from services defined under “Network -> DHCP”.

## **Anti-Virus Update**

The update log contains notifications regarding the start and progress of the virus signature file update process.

## **SNMP/LLDP**

Messages from services defined under “Management -> SNMP”.

## **IPsec VPN**

Lists all VPN events.

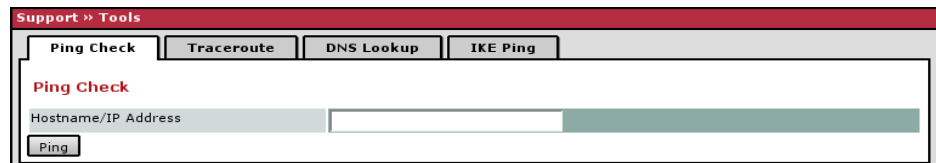
The format corresponds to the standard Linux format.

It offers special evaluation programs that present information from the logged data in a more readable format.

## 6.14 Support Menu

### 6.14.1 *Support* → *Tools*

#### Ping Check

The screenshot shows a web interface titled "Support >> Tools". It has four tabs: "Ping Check", "Traceroute", "DNS Lookup", and "IKE Ping". The "Ping Check" tab is active. Below the tabs, there is a section titled "Ping Check" in red. It contains a text input field labeled "Hostname/IP Address" and a "Ping" button.

#### Ping Check

Goal:

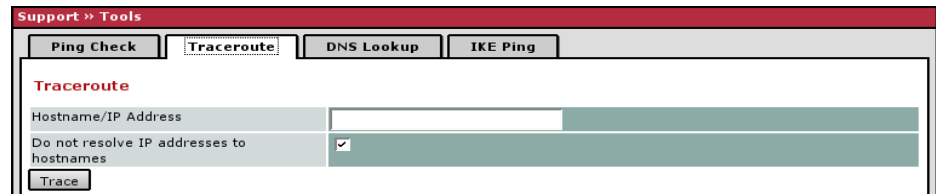
To check if the remote peer is accessible over a network.

Procedure:

Enter the IP address or remote peer hostname in the **Hostname/IP Address** field. Click on the **Ping** button.

You will then receive an appropriate notification.

#### Traceroute

The screenshot shows a web interface titled "Support >> Tools". It has four tabs: "Ping Check", "Traceroute", "DNS Lookup", and "IKE Ping". The "Traceroute" tab is active. Below the tabs, there is a section titled "Traceroute" in red. It contains a text input field labeled "Hostname/IP Address", a checkbox labeled "Do not resolve IP addresses to hostnames" which is checked, and a "Trace" button.

#### Traceroute

Goal:

To establish which intermediary peers or routers are found on the connection path to a remote peer computer.

Procedure:

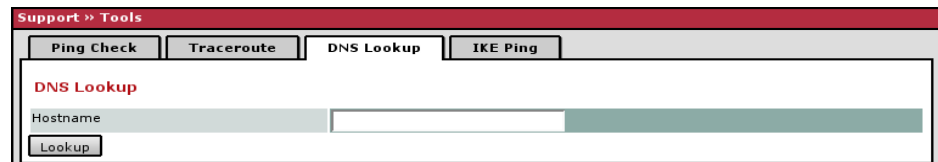
Enter the remote peer IP address or hostname where the route is to be calculated in the **Hostname/IP Address** field.

If the points on the route are to be given with IP addresses and not hostnames (if applicable), activate the **Do not resolve IP addresses to hostnames** checkbox.

Click on the **Trace** button.

You will then receive an appropriate notification.

## DNS Lookup



The screenshot shows a web interface for the 'Support >> Tools' section. There are four tabs: 'Ping Check', 'Traceroute', 'DNS Lookup', and 'IKE Ping'. The 'DNS Lookup' tab is selected. Below the tabs, the title 'DNS Lookup' is displayed in red. There is a text input field labeled 'Hostname' and a 'Lookup' button below it.

### DNS Lookup

Goal:

To establish  
which hostname belongs to a certain IP address  
OR  
which IP address belongs to a certain hostname.

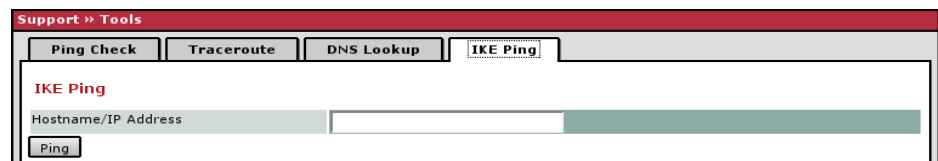
Procedure:

Enter the IP address or hostname in the **Hostname** field.

Click on the **Lookup** button.

You will then receive the answer defined by the mGuard according to the DNS configuration.

## IKE Ping



The screenshot shows a web interface for the 'Support >> Tools' section. There are four tabs: 'Ping Check', 'Traceroute', 'DNS Lookup', and 'IKE Ping'. The 'IKE Ping' tab is selected. Below the tabs, the title 'IKE Ping' is displayed in red. There is a text input field labeled 'Hostname/IP Address' and a 'Ping' button below it.

### IKE Ping

Goal:

To determine if the VPN gateway software is able to establish a VPN connection, or if a firewall prevents this.

Procedure:

Enter the name or IP address of the VPN gateway in the **Hostname/IP Address** field.

Click on the **Ping** button.

You will then receive an appropriate notification.

## 6.14.2 Support → Advanced

### Hardware

Support > Advanced	
Hardware	Snapshot
<b>Hardware Information</b>	
Hardware	Innominate mGuard
CPU	XScale-IXP42x Family rev 1 (v5b)
CPU Family	IXP4XX
CPU Stepping	B0
CPU Clock Speed	533 MHz
System Uptime	18:23
User Space Memory	62568 kB
MAC 1	00:0c:be:02:20:cf
MAC 2	00:0c:be:02:20:d0
Product Name	Innominate mGuard
OEM Name	Innominate
OEM Serial Number	2T900054
Serial Number	2T900054
Flash ID	00040001413e1dd1
Hardware Version	000007dc
Version Parameterset	2

This page lists the hardware properties of the mGuard.

### Snapshot

Support > Advanced	
Hardware	Snapshot
<b>Support Snapshot</b>	
<input type="button" value="Download"/>	
This will create a snapshot of the mGuard for support purposes.	

This function is used for support purposes.

It creates a compressed file (in tar.gz format) containing all current configuration settings and log entries that could be relevant to error diagnosis.

☒ This file does not contain any private information such as the private machine certificate or passwords. However, any Pre-Shared Keys of VPN connections are contained in snapshots.

To create a snapshot, please proceed as follows:

1. Click on **Download**.
2. Save the file (under the name snapshot.tar.gz).

Provide the file for support purposes, if required.

## 6.15 CIDR (Classless Inter-Domain Routing)

IP netmasks and CIDR are notations that combine several IP addresses into one address space. In this case, an address space with sequential addresses is treated as a network.

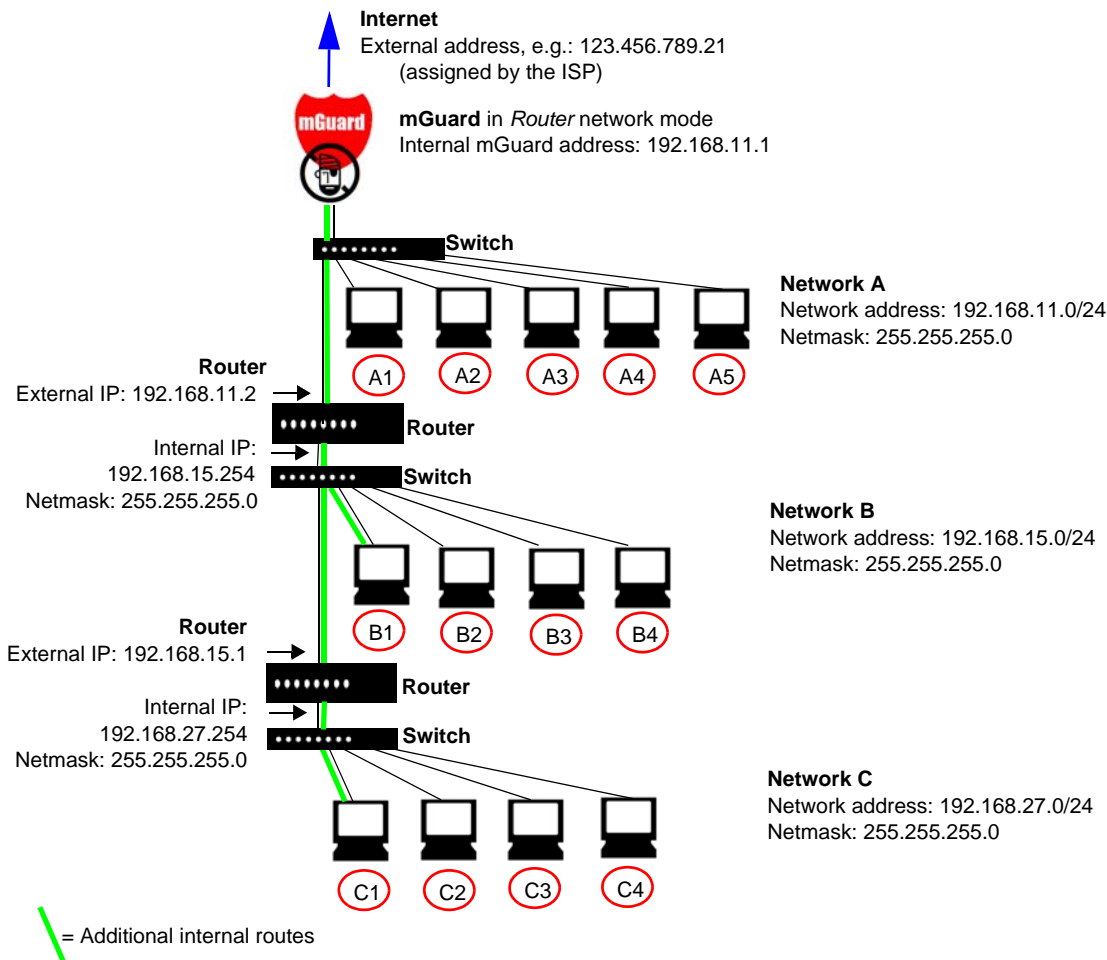
To define a range of IP addresses for the mGuard (e.g. when configuring the firewall), it may be necessary to use CIDR notation to specify the address space. The following table shows the IP netmask on the left and the corresponding CIDR notation on the right.

IP netmask	Binary				CIDR
255.255.255.255	11111111	11111111	11111111	11111111	32
255.255.255.254	11111111	11111111	11111111	11111110	31
255.255.255.252	11111111	11111111	11111111	11111100	30
255.255.255.248	11111111	11111111	11111111	11111000	29
255.255.255.240	11111111	11111111	11111111	11110000	28
255.255.255.224	11111111	11111111	11111111	11100000	27
255.255.255.192	11111111	11111111	11111111	11000000	26
255.255.255.128	11111111	11111111	11111111	10000000	25
255.255.255.0	11111111	11111111	11111111	00000000	24
255.255.254.0	11111111	11111111	11111110	00000000	23
255.255.252.0	11111111	11111111	11111100	00000000	22
255.255.248.0	11111111	11111111	11111000	00000000	21
255.255.240.0	11111111	11111111	11110000	00000000	20
255.255.224.0	11111111	11111111	11100000	00000000	19
255.255.192.0	11111111	11111111	11000000	00000000	18
255.255.128.0	11111111	11111111	10000000	00000000	17
255.255.0.0	11111111	11111111	00000000	00000000	16
255.254.0.0	11111111	11111110	00000000	00000000	15
255.252.0.0	11111111	11111100	00000000	00000000	14
255.248.0.0	11111111	11111000	00000000	00000000	13
255.240.0.0	11111111	11110000	00000000	00000000	12
255.224.0.0	11111111	11100000	00000000	00000000	11
255.192.0.0	11111111	11000000	00000000	00000000	10
255.128.0.0	11111111	10000000	00000000	00000000	9
255.0.0.0	11111111	00000000	00000000	00000000	8
254.0.0.0	11111110	00000000	00000000	00000000	7
252.0.0.0	11111100	00000000	00000000	00000000	6
248.0.0.0	11111000	00000000	00000000	00000000	5
240.0.0.0	11110000	00000000	00000000	00000000	4
224.0.0.0	11100000	00000000	00000000	00000000	3
192.0.0.0	11000000	00000000	00000000	00000000	2
128.0.0.0	10000000	00000000	00000000	00000000	1
0.0.0.0	00000000	00000000	00000000	00000000	0

Example: 192.168.1.0 / 255.255.255.0 corresponds to CIDR: 192.168.1.0/24

6.16 Network Example

The following sketch illustrates how IP addresses can be distributed in a local network with subnetworks, which network addresses result and how the details regarding additional internal routes may look.



Network A

Computer	A1	A2	A3	A4	A5
IP address	192.168.11.3	192.168.11.4	192.168.11.5	192.168.11.6	192.168.11.7
Netmask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0

Network B

Computer	B1	B2	B3	B4
IP address	192.168.15.2	192.168.15.3	192.168.15.4	192.168.15.5
Netmask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0

**Additional internal routes:**  
Network: 192.168.15.0/24  
Gateway: 192.168.11.2

Network C

Computer	C1	C2	C3	C4
IP address	192.168.27.1	192.168.27.2	192.168.27.3	192.168.27.4
Netmask	255.255.255.0	255.255.255.0	255.255.255.0	255.255.255.0

Network: 192.168.27.0/24  
Gateway: 192.168.11.2

## 7 The Rescue Button – Restarting, the Recovery Procedure and Flashing Firmware

The Rescue button is used to perform the following procedures:

### 7.1 Performing a restart



**Objective** To restart the device with the configured settings.

**Action:** Press the **Rescue button** for approx. 1.5 seconds:

- mGuard industrial RS: Until the error LED lights up
- smart: Until the middle LED lights up red
- blade, PCI: Until both red LEDs light up
- EAGLE mGuard: Until the status LED and the link LEDs are extinguished
- delta: Until the status LED stops blinking

OR

- Briefly disconnect the power supply
- mGuard PCI: Restart the computer where the mGuard PCI card is installed

### 7.2 Performing a recovery



**Objective** To reset the network configurations to the factory defaults, as it is no longer possible to access the mGuard:  
All mGuard versions (except the mGuard delta and blade controller) in *Stealth* mode (autodetect) with the IP address 1.1.1.1.  
The mGuard delta and mGuard blade controller in *Router* mode with the IP address 192.168.1.1.

Furthermore, MAU management for ethernet connections is switched on and HTTPS is approved for use on the local ethernet connection (LAN).

☒ The passwords, configured settings for VPN connections and the firewall are all retained.

**Possible reasons for starting the Recovery procedure:**

The mGuard is in Router or PPPoE mode

- The mGuard device address has been changed from the default setting
- The current IP address of the device is unknown

- Action:**
1. Press the **Rescue** button slowly 6 times.
  2. The mGuard responds after about two seconds:
    - mGuard industrial RS
      - If successful, the state LED lights up green
      - If unsuccessful, the error LED lights up red
    - smart
      - If successful, the middle LED lights up green
      - If unsuccessful, the middle LED lights up red
    - blade, PCI
      - If successful, the LAN LED lights up red
      - If unsuccessful, the WAN LED lights up red
    - EAGLE mGuard
      - If successful, the status LED lights up yellow
      - If unsuccessful, the error LED lights up red
    - mGuard delta
      - If successful, the status LED lights up green
      - If unsuccessful, the status LED stays off
  3. Once again, press the **Rescue** button slowly 6 times.
  4. If successful, the device reboots after two seconds and switches to *Stealth* mode (or Router mode for mGuard delta and blade controller). It can then be accessed again under the following address: **https://1.1.1.1/** (mGuard delta and blade controller: **https://192.168.1.1/**).

## 7.3 Flashing the firmware



**Objective** To reload all mGuard software onto the device.

- ☒ **All configured settings are deleted.** The mGuard is restored to the factory default settings.  
From mGuard version 5.0.0 onwards, the licenses installed in the mGuard remain in place after flashing the firmware. They therefore do not need to be installed again.
- ☒ Only firmware from version 5.1.0 onwards can be installed on the mGuard industrial RS.

**Possible reasons for flashing the firmware:**

- The administrator and root password have been lost.

**Action:** Proceed as follows:

- ☒ **Do not disconnect the power supply to the mGuard during the flashing procedure! The device could be damaged and may be left inoperable. This will require the device to be reactivated by the manufacturer.**

**Requirements:**

- The mGuard software has been obtained from Innominate Support or downloaded from Innominate's web site [www.innominate.com](http://www.innominate.com) and saved on the configuration computer.
- If your current software version is higher than the factory default of the device, then you must obtain the relevant license for using this update. This applies to major release upgrades, for example from version 4.x.x to version 5.x.x to version 6.x.x etc.

- The DHCP and TFTP servers can both be accessed under the same IP address – see “Requirements for flashing the firmware: DHCP and TFTP server” on page 251.
- mGuard PCI: When the mGuard is operated in Power-over-PCI mode, the DHCP / TFTP server must be connected to the mGuard's LAN socket. When the mGuard is operated in PCI Driver mode, the DHCP/TFTP server must be operated on the computer or operating system provided by the interface to the mGuard.

1. Keep the **Rescue** button pressed until the *Recovery* status is entered as follows:

The mGuard is restarted (after approx. 1.5 seconds). After another 1.5 seconds the mGuard enters the *Recovery* status mode:

- mGuard industrial RS: The state, LAN and WAN LEDs light up green
- smart: All LEDs light up green
- blade, PCI: The green and red LAN LEDs light up
- EAGLE mGuard: The 1, 2 and V.24 LEDs light up
- delta: The status LED fades slowly

2. Release the **Rescue** button not later than one second after the *Recovery* status is reached. The mGuard restarts if the **Rescue** button is not released quickly enough.

The mGuard will now start the Recovery system: It searches for a DHCP server over the LAN port in order to obtain an IP address.

- Status display:
  - mGuard industrial RS: The state LED flashes
  - smart: The middle LED (heartbeat) flashes
  - blade, PCI: The red LAN LED flashes
  - EAGLE mGuard: The 1, 2 and V.24 LEDs light up orange
  - delta: The status LED flashes

The “install.p7s” file is loaded from the TFTP server. This contains the electronically authenticated control procedure for the installation process. Only files signed by Innominate are accepted.

The control procedure now deletes the current flash memory contents and prepares for a new software installation.

- Status display:
  - mGuard industrial RS: The modem, state and LAN LEDs form a light sequence
  - smart: The three green LEDs form a light sequence
  - blade, PCI: The green and red LAN LEDs form a light sequence
  - EAGLE mGuard: The 1, 2 and V.24 LEDs form a light sequence
  - delta: The status LED flashes at a faster rate

The “jffs2.img.p7s” file is downloaded from the TFTP server and written onto the flash memory. This file contains the actual mGuard operating system and is signed electronically. Only files signed by Innominate will be accepted. This process takes around 3 to 5 minutes.

- Status display:
  - mGuard industrial RS: The state LED lights up continuously
  - smart: The middle LED (heartbeat) lights up continuously
  - blade, PCI: The green LEDs and red LAN LED flash continuously

- EAGLE mGuard: The 1, 2 and V.24 LEDs are out, the p1, p2 and status LEDs light up green continuously
- delta: The status LED lights up continuously

The new software is unpacked and configured. This takes approximately 20 minutes.

As soon as the procedure has been completed:

- mGuard industrial RS: The modem, state and LAN LEDs flash green simultaneously
- smart: All three LEDs light up green continuously and at the same time
- blade, PCI: The mGuard restarts
- EAGLE mGuard: The 1, 2 and V.24 LEDs light up green continuously and at the same time
- delta: The status LED flashes once per second

3. Restart the mGuard (not necessary for blade and PCI).

To do this, press the **Rescue** button briefly.

OR

Disconnect the power supply and then connect again (for smart: using a USB cable used as a power supply only).

Result:

The mGuard is restored to its factory settings. You can now configure it once again – see “Setting up a local configuration connection” on page 52.

**Requirements for flashing the firmware: DHCP and TFTP server**

To flash firmware, a DHCP and TFTP server must be installed on the locally connected system.

(DHCP = **D**ynamic **H**ost Configuration **P**rotocol; TFTP = **T**rivial **F**ile **T**ransfer **P**rotocol)

Install the DHCP and TFTP server, if necessary (see below).

⊠ The installation of a second DHCP server in a network can affect the configuration of the entire network!

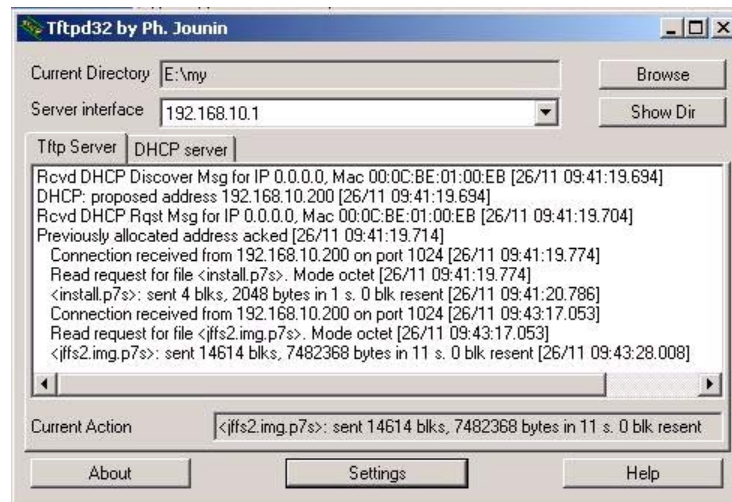
### 7.3.1 Installing DHCP and TFTP servers in Windows or Linux

#### In Windows

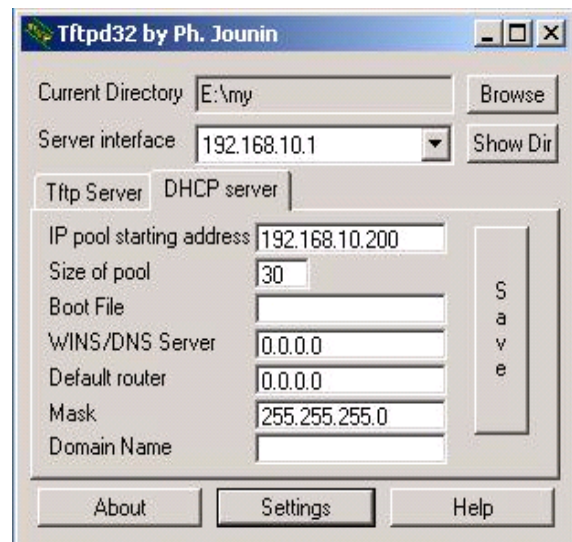
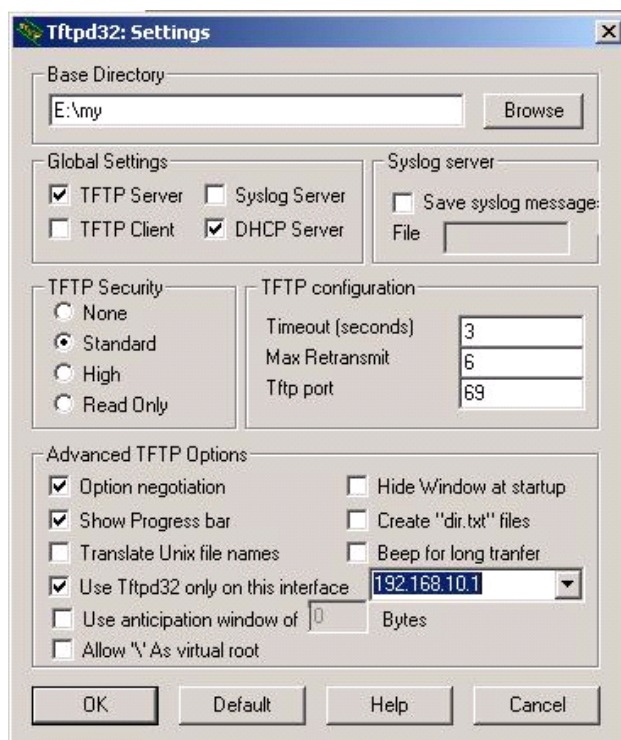
Install the program which can be found in the download section of Innominate's homepage [www.innominate.com](http://www.innominate.com). To do this, proceed as follows:

1. Disconnect the Windows computer from all networks.
2. Copy the software into any empty folder on the Windows computer. Start the TFTP32.EXE program.
3. The set host IP is: **192.168.10.1**. This must also be the network card address. Click on the **Browse** button to switch to the folder where the mGuard image files have been saved: **install.p7s, jffs2.img.p7s**

If a major release upgrade of the firmware is carried out due to the flash procedure, the license file purchased for the update must also be stored here under the name **licence.lic**. Please ensure that this is the correct license for the device (see "Management → Update" on page 82).



4. Click on the *Tftp Server* or *DHCP Server* tab and then click on the **Settings** button. Set the parameters as shown below:



## In Linux

All current Linux distributions include DHCP and TFTP servers. Install the corresponding packages as described in the instructions for the respective distributions.

Configure the DHCP server by making the following settings in the **/etc/dhcpd.conf** field:

```
subnet 192.168.134.0 netmask 255.255.255.0 {  
  range 192.168.134.100 192.168.134.119;  
  option routers 192.168.134.1;  
  option subnet-mask 255.255.255.0;  
  option broadcast-address 192.168.134.255;}
```

This sample configuration makes 20 IP addresses (.100 to .119) available. It is assumed that the DHCP server has the address 192.168.134.1 (settings for ISC DHCP 2.0).

The required TFTP server is configured in the following file:

**/etc/inetd.conf**

In this file, insert the appropriate lines or set the necessary parameter for TFTP service. (The directory for the data is: **/tftpboot**):

```
tftp dgram udp wait root /usr/sbin/in.tftpd -s /tftpboot/
```

The mGuard image files must be saved in the **/tftpboot** directory:

**install.p7s, jffs2.img.p7s**

If a major release upgrade of the firmware is carried out due to the flash procedure, the license file purchased for the update must also be stored here under the name **licence.lic**. Please ensure that this is the correct license for the device (see “Management → Update” on page 82).

Restart the “inetd” process again to activate the modified configuration.

If you use a different process (e.g. xinetd), please consult the appropriate documentation.

## 8 Glossary

### **Asymmetrical encryption**

In asymmetrical encryption, data is encrypted with one key and decrypted with a second key. Both keys are suitable for encryption and decryption. One of the keys is kept secret by its owner (Private Key), whilst the other is made available to the public (Public Key), i.e. to possible communication partners.

A message encrypted with the public key can only be decrypted and read by the owner of the associated private key. A message encrypted with the private key can be decrypted by any recipient who is the owner of the associated public key. Encryption using the private key shows that the message actually originated from the owner of the associated public key. Therefore, the expression “digital signature” is also often used.

However, asymmetrical encryption techniques such as RSA are both slow and susceptible to certain types of attack, meaning they are often combined with some form of symmetrical encryption (→ Symmetrical encryption). On the other hand, concepts are available which avoid the additional administration of symmetrical keys.

### **DES / 3DES**

This symmetrical encryption algorithm was developed by IBM and checked by the NSA. DES (→ Symmetrical encryption) was set in 1977 by the American National Bureau of Standards, which was the predecessor of the National Institute of Standards and Technology (NIST), as the standard for American governmental institutions. As this was the very first standardized encryption algorithm, it quickly won acceptance in industrial circles, both inside and outside America.

DES uses a 56 bit key length, which is no longer considered secure as the available processing power has greatly increased since 1977.

3DES is a variant of DES. It uses keys that are three times as long, i.e. 168 bits long. This is still considered to be secure and is also included in the IPsec standard.

### **AES**

The AES (Advanced Encryption Standard) was developed by NIST (National Institute of Standards and Technology) in cooperation with the industry.

This → symmetrical encryption standard was developed to replace the earlier DES standard. AES specifies three different key lengths (128, 192 and 256 bits).

In 1997, NIST started the AES initiative and announced its conditions for the algorithm. From the many proposed encryption algorithms, NIST selected a total of five algorithms for closer examination – the MARS, RC6, Rijndael, Serpent and Twofish algorithms. In October 2000, the Rijndael algorithm was adopted as the encryption algorithm.

### **CA certificate**

Used to check the reliability of a CA certificate and the CA (Certificate Authority) that issued it (→ X.509 certificate). A CA certificate can be consulted in order to check that a certificate signature has this CA. This check only makes sense if there is little doubt that the CA certificate originates from an authentic source (i.e. is also authentic). If doubt occurs, then the CA certificate itself can be checked. If (as is usually the case) this applies to a sub-CA certificate (i.e. a CA certificate issued by a sub-certificate authority), then the CA certificate of the superordinate CA can be used to check the CA certificate of the subordinate instance. If a superordinate CA certificate also has a superordinate CA certificate, then its CA certificate can be used to check the CA certificate of the subordinate instance. This chain of trust continues down to the root instance (root CA). The CA file of the root CA is necessarily self-signed. This instance is the highest available, and is ultimately the basis of trust.

No-one else can certify that this instance is actually the instance in question. A root CA is therefore a state or state-controlled organization. The mGuard can use its imported CA certificate to check the validity of displayed certificates from remote peers. For example, with VPN connections the authentication of remote peers can only be made using the CA certificate. In this case, all CA certificates must be installed in mGuard in order to build a chain with the certificate displayed by the remote peer: Aside from the CA certificate, whose signature can be seen in the displayed certificate of the VPN partner to be checked, the CA certificate of the superordinate CA up to the root certificate must also be used. If this “trust chain” is checked meticulously in order to accept the authenticity of a remote peer, then the level of security increases.

**Client / Server**

In a client-server environment, a server is a program or computer which accepts and answers queries from client programs or computers. In data communication, the computer which establishes a connection to a server (or host) is also called a client. In other words, the client is the calling computer and the server (or host) is the computer called.

**Datagram**

In the IP protocol, data is sent in the form of data packets. These are known as IP datagrams. An IP datagram has the following structure:

IP Header	TCP, UDP, ESP etc. Header	Data (Payload)
-----------	---------------------------	----------------

The IP header contains:

- The IP address of the sender (source IP address)
- The IP address of the recipient (destination IP address)
- The protocol number of the protocol on the superordinate protocol layer (according to the OSI layer model)
- The IP header checksum used to check the integrity of the received header.

The TCP/UDP header contains the following information:

- The sender’s port (source port)
- The recipient’s port (destination port)
- A checksum covering the TCP header and information from the IP header (e.g. source and destination IP addresses)

**Default route**

If a computer is connected to a network, the operating system creates a routing table internally. It lists the IP addresses that the operating system has identified based on the connected computers and the routes available at that moment. The routing table thus contains the possible routes (destinations) for sending IP packets. If IP packets are to be sent, the computer’s operating system compares the IP addresses stated in the IP packets with the entries in the routing table in order to determine the correct route.

If a router is connected to the computer and its internal IP address (i. e. the IP address of the router’s LAN port) has been relayed to the operating system as the standard gateway (in the network card’s TCP/IP configuration), then this IP address is used as the destination if all other IP addresses in the routing table are not suitable. In this case the IP address of the router specifies the default route, because all IP packets (by default = standard) whose IP address have no counterpart in the routing table (i. e. cannot find a route) are directed to this gateway.

**DynDNS provider**

Also known as *Dynamic DNS provider*. Every computer connected to the Internet has an IP address (IP = Internet Protocol). If the computer accesses the Internet via a dial-up modem, ISDN or ADSL, its ISP will assign it a dynamic IP address. In other words, the address changes for each online session. Even if the computer is online 24 hours a day without interruption (e.g. flat-rate), the IP address will change during the session.

If a local computer should be accessible via the Internet, it must have an address that is known to the remote peer. This is the only way to establish a connection to the local computer. If the address of the local computer changes constantly, then this is not possible. The exception to this is when the operator of the local computer has an account with a Dynamic DNS provider (DNS = Domain Name Server).

In this case, the operator can set a host name with this provider under which the system should be accessible, e.g. `www.example.com`. The Dynamic DNS provider also provides a small program that must be installed and run on the affected computer. At each new Internet session, this tool informs the Dynamic DNS provider which IP address the local computer has currently been assigned. The Domain Name Server registers the current assignment of host name to IP address and also informs the other Domain Name Servers over the Internet.

If a remote system now wishes to establish a connection to a local system that is registered with the DynDNS provider, then the remote system can use the host name of the local system as its address. This will establish a connection to the responsible DNS (Domain Name Server) in order to look up the IP address that is currently registered for this host name. The corresponding IP address is sent back from the DNS to the remote system, which can then use this as the destination address. This now leads directly to the desired local computer.

In principle, all Internet addresses are based on this procedure: First, a connection to a DNS is established in order to determine the IP address assigned for the host name. Once this has been accomplished, the established IP address is used to set up a connection to the desired remote peer, which could be any site on the Internet.

**IP address**

Every host or router on the Internet / intranet has a unique IP address (IP = Internet Protocol). An IP address is 32 bits (= 4 bytes) long and is written as four numbers (each from 0 to 255), which are separated by a dot.

An IP address consists of 2 parts: the network address and the host address.

Network Address	Host Address
-----------------	--------------

All network hosts have the same network address, but different host addresses. The two parts of the address differ in length depending on the size of the respective network (networks are categorized as Class A, B or C).

	1. Byte	2. Byte	3. Byte	4. Byte
<b>Class A</b>	Network Address	Host Address		
<b>Class B</b>	Network Address		Host Address	
<b>Class C</b>	Network Address			Host Address

The first byte of the IP address determines whether the IP address of a network device belongs to Class A, B or C. The following has been specified:

	Value of 1st byte	No. of the bytes for the network address	No. of bytes for the host address
<b>Class A</b>	1 - 126	1	3
<b>Class B</b>	128 - 191	2	2
<b>Class C</b>	192 - 223	3	1

There is thus a maximum worldwide total of 126 Class A networks. Each of these networks can have a maximum of  $256 \times 256 \times 256$  hosts (3 bytes of address space). There can be  $64 \times 256$  Class B networks and each of these networks can have up to 65,536 hosts (2 bytes address space:  $256 \times 256$ ). There can be  $32 \times 256 \times 256$  Class C networks and each of these networks can have up to 256 hosts (1 byte address space).

### Subnet mask

Normally, a company network with access to the Internet is only officially assigned a single IP address, e.g. 123.456.789.21. Based on the first byte of this sample address, one can see that this company network is a Class B network. This means that the last 2 bytes are free to be used for host addresses. This produces an address space for up to 65,536 possible hosts ( $256 \times 256$ ).

Such a huge network is not practical. There is a need to build subnetworks here. The subnet mask can be used for this. Like an IP address, this mask is 4 bytes long. The bytes that represent the network address are each assigned the value 255. This can mainly be used to “borrow” a portion of the host address that can then be used to address the subnetworks. In this example, by using the subnet mask 255.255.255.0 in a Class B network (2 bytes for the network address, 2 bytes for the host address), the third byte, which was actually intended for host addressing, can now be used for subnet addressing. With this configuration, the company network could support 256 subnetworks that each have 256 hosts.

## IPsec

IP Security (IPsec) is a standard that uses encryption to verify the authenticity of the sender and to ensure the confidentiality and integrity of the data in IP datagrams (→Datagram). The components of IPsec are the Authentication Header (AH), the Encapsulating Security Payload (ESP), the Security Association (SA) and the Internet Key Exchange (IKE).

At the start of the session, systems that wish to communicate must determine which technique should be used and the implications of this choice for the session e.g. *Transport Mode* or *Tunnel Mode*.

In *Transport Mode*, an IPsec header is inserted between the IP header and the TCP or UDP header respectively in each IP datagram. Since the IP header remains unchanged, this mode is only suitable for host-to-host connections.

In *Tunnel Mode*, an IPsec header and a new IP header are added in front of the entire IP datagram. This means the original datagram is encrypted in its entirety and stored in the payload of the new datagram.

The *Tunnel Mode* is used in VPN applications: The devices at the tunnel ends ensure that the datagrams are encrypted before they pass through the tunnel. This means the actual datagrams are completely protected whilst being transferred over a public network.

**Subject, certificate**

In a certificate, the classification of a certificate to its owner is confirmed by a CA (Certificate Authority). This occurs through the confirmation of certain owner characteristics. Furthermore, the certificate owner must possess the private key that matches the public key in the certificate (→ X.509 certificate).

Example:

```
Certificate:
Data:
  Version: 3 (0x2)
  Serial Number: 1 (0x1)
  Signature Algorithm: md5WithRSAEncryption
  Issuer: C=XY, ST=Austria, L=Graz, O=TrustMe Ltd, OU=Certificate Authority, CN=CA/Email=ca@trustme.dom
  Validity
    Not Before: Oct 29 17:39:10 2000 GMT
    Not After: Oct 29 17:39:10 2000 GMT
  Subject: CN=anywhere.com, E=doctrans.de, C=DE, ST=Hamburg, L=Hamburg, O=Innominate, OU=Security
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (1024 bit)
      Modulus (1024 bit):
        00:c4:40:4c:6e:14:1b:61:36:84:24:b2:61:c0:b5:
        d7:e4:7a:a5:4b:94:ef:d9:5e:43:7f:c1:64:80:fd:
        9f:50:41:6b:70:73:80:48:90:f3:58:bf:f0:4c:b9:
        90:32:81:59:18:16:3f:19:f4:5f:11:68:36:85:f6:
        1c:a9:af:fa:a9:a8:7b:44:85:79:b5:f1:20:d3:25:
        7d:1c:de:68:15:0c:b6:bc:59:46:0a:d8:99:4e:07:
        50:0a:5d:83:61:d4:db:c9:7d:c3:2e:eb:0a:8f:62:
        8f:7e:00:e1:37:67:3f:36:d5:04:36:44:44:77:e9:
        f0:b4:95:f5:f9:34:9f:f8:43
      Exponent: 65537 (0x10001)
  X509v3 extensions:
    X509v3 Subject Alternative Name:
      email:xyz@anywhere.com
    Netscape Comment:
      mod_ssl generated test server certificate
    Netscape Cert Type:
      SSL Server
  Signature Algorithm: md5WithRSAEncryption
  12:ed:f7:b3:5e:a0:93:3f:a0:1d:60:cb:47:19:7d:15:59:9b:
  3b:2c:a8:a3:6a:03:43:d0:85:d3:86:86:2f:e3:aa:79:39:e7:
  82:20:ed:f4:11:85:a3:41:5e:5c:8d:36:a2:71:b6:6a:08:f9:
  cc:1e:da:c4:78:05:75:8f:9b:10:f0:15:f0:9e:67:a0:4e:a1:
  4d:3f:16:4c:9b:19:56:6a:f2:af:89:54:52:4a:06:34:42:0d:
  d5:40:25:6b:b0:c0:a2:03:18:cd:d1:07:20:b6:e5:c5:1e:21:
  44:e7:c5:09:d2:d5:94:9d:6c:13:07:2f:3b:7c:4c:64:90:bf:
  ff:8e
```

The *Subject Distinguished Name*, or *Subject*, clearly identifies the certificate owner. The entry is comprised of several components. These are known as attributes (see example certificate above). The following table contains a list of possible attributes. The sequence of attributes in a X.509 certificate can vary.

Abbreviation	Name	Explanation
CN	Common Name	Identifies the person or object that the certificate belongs to. Example: CN=server1
E	Email address	Shows the email address of the certificate owner.
OU	Organizational Unit	Shows the department within an organization or company. Example: O=Development
O	Organization	Shows the organization or company. Example: O=Innominate
L	Locality	Shows the place / locality Example: L=Hamburg
ST	State	Shows the federal state / county. Example: ST=Bavaria

Abbreviation	Name	Explanation
C	Country	Two-letter code that identifies the country (Germany=DE) Example: C=DE

A filter can be set for the subject (i.e. certificate owner) during VPN connections and remote service access to the mGuard by SSH or HTTPS. After this, only certificates from remote peers are accepted that have certain attributes in the subject line.

### NAT (Network Address Translation)

During Network Address Translation (NAT) (also known as *IP Masquerading*), an entire network is “hidden” behind a single device, known as a NAT router. If you communicate externally via a NAT router, the internal computers in the local network and their IP addresses remain hidden. The remote communication partner will only see the NAT router with its own IP address.

In order to allow internal computers to communicate directly with external systems (over the Internet), the NAT router must modify the IP datagrams that are passed to and from the internal computers and the remote peers.

If an IP datagram is sent from the internal network to a remote peer, the NAT router modifies the UDP and TCP headers of the datagram. It replaces the source IP address and port with its own IP address and an unused port. A table is stored in which the original values are listed together with the corresponding new ones.

When a reply datagram is received, the NAT router will recognize that it is intended for an internal computer using the destination port of the datagram.

Using the table, the NAT router will replace the destination IP address and port and then forward the datagram on via the internal network.

### Port number

A port number is assigned to each UDP and TCP protocol participant. It is then possible to differentiate two UDP or TCP connections between two systems and use them at the same time.

Fixed port numbers can be reserved for special purposes. For example, HTTP connections are usually assigned to TCP port 80 and POP3 connections to port 110.

### Proxy

A proxy is an intermediary service. A web proxy (e. g. Squid) is often used for a large network. For example, if 100 employees access a certain website at the same time over a web proxy, then the proxy only loads the relevant web pages once from the server and then distributes them as needed amongst the employees. Remote web traffic is reduced, which saves money.

### PPPoE

PPPoE is an acronym of **P**oint-to-**P**oint **P**rotocol over **E**thernet. This protocol is based on PPP and ethernet standards. PPPoE defines how to connect users via ethernet with the Internet via a jointly used broadband medium such as DSL, wireless LAN or a cable modem.

### PPTP

PPTP is an acronym of **P**oint-to-**P**oint **T**unneling **P**rotocol. This protocol was developed by companies such as Microsoft and U.S. Robotics in order to securely transfer data between VPN nodes (→ VPN) via a public network.

### Router

A router is a device that is connected to different IP networks and communicates between them. To do this, a router has an interface for each network connected to it. A router must find the correct path to the target for incoming data and must define the appropriate interface for forwarding it. It takes data from a local

routing table that shows which networks are available over which router connections (or intermediary stations).

**Trap**

Aside from other protocols, an SNMP (Simple Network Management Protocol) can also be used, especially in large networks. This UDP-based protocol is used for the central administration of network devices. For example, the configuration of a device can be requested using the “GET” order and changed using the “SET” order. To do this, the requested network device must be SNMP compatible. An SNMP compatible device can also send SNMP messages (e. g. when unexpected events occur). Messages of this kind are known as SNMP traps.

**X.509 certificate**

A type of “seal” that certifies the authenticity of a public key (→ Asymmetrical encryption) and the associated data.

It is possible to use certification to enable the user of the public key (used to encrypt the data) to ensure that the received public key is from its actual issuer (and thus from the instance that should later receive the data). A *Certification Authority (CA)* certifies the authenticity of the public key and the associated link between the identity of the issuer and their key. The certification authority will verify authenticity in accordance with its rules. For example, this may require the issuer of the public key to appear before it in person. Once successfully authenticated, the CA adds its digital signature to the issuer’s public key. This results in a certificate.

An X.509(v3) certificate is thus comprised of a public key, information about the key owner (given as Distinguished Name (DN)), authorized usage etc. and the signature of the CA (→ Subject, certificate).

The signature is created as follows: The CA creates an individual bit sequence, known as the HASH value, from the bit sequence of the public key, owner information and other data. This sequence may be up to 160 bits long. The CA then encrypts this with its own private key and then adds it to the certificate. The encryption with the CA's private key proves the authenticity of the certificate (i.e. the encrypted HASH string is the CA's digital signature). If the certificate data is altered, then this HASH value will no longer be correct and the certificate is then worthless.

The HASH value is also known as the fingerprint. Since it is encrypted with the CA's private key, anyone who has the corresponding public key can decrypt the bit sequence and thus verify the authenticity of the fingerprint or signature.

The usage of a certification authority means it is not necessary for key owners to know each other. They must only know the certification authority used in the process. The additional key information further simplifies administration of the key.

X.509 certificates can be used for email encryption with S/MIME or IPsec.

**Protocol, communication protocol**

Devices that communicate with each other must follow the same rules. To do this, they must “speak” the same language. Rules and standards of this kind are called protocols or communication protocols. Some of the more frequently used protocols are IP, TCP, PPP, HTTP and SMTP.

**Service provider**

Service providers are companies or institutions that enable users to access the Internet or online services.

**Spoofing, anti-spoofing**

In Internet terminology, spoofing means supplying a false address. Using this false Internet address, a user can create the illusion of being an authorized user. Anti-spoofing is the term for mechanisms that detect or prevent spoofing.

**Symmetrical encryption**

In symmetrical encryption, the same key is used to encrypt and decrypt data. Two examples of symmetrical encryption algorithms are DES and AES. They are fast, but also difficult to administrate as the number of users increases.

**TCP/IP  
(Transmission  
Control Protocol/  
Internet Protocol)**

These are network protocols used to connect two computers over the Internet. IP is the base protocol.

UDP is based on IP and sends individual packets. The packets may arrive at the recipient in a different order in which they were sent or they may even be lost. TCP is used for connection security and ensures, for example, that data packets are passed on to the application in the correct order.

UDP and TCP add port numbers between 1 to 65535 to the IP addresses.

These distinguish the various services offered by the protocols.

A number of additional protocols are based on UDP and TCP, e.g. HTTP (HyperText Transfer Protocol), HTTPS (Secure HyperText Transfer Protocol), SMTP (Simple Mail Transfer Protocol), POP3 (Post Office Protocol, Version 3) and DNS (Domain Name Service).

ICMP is based on IP and contains control messages.

SMTP is an email protocol based on TCP.

IKE is an IPsec protocol based on UDP.

ESP is an IPsec protocol based on IP.

On a Windows PC, the WINSOCK.DLL (or WSOCK32.DLL) handles the development of both protocols.

(→ Datagram)

**VLAN**

A VLAN (Virtual Local Area Network) divides a physical network into several independent logical networks.

Devices of different VLANs can only access devices within their own VLAN. Assignment to a VLAN is no longer defined by the network topology alone, but also by the configured VLAN ID.

VLAN settings can also be used as optional settings for each IP. A VLAN is identified by its VLAN ID (1-4094). All devices with the same VLAN ID belong to the same VLAN and can therefore communicate with each other.

The ethernet packet for a VLAN (based on IEEE 802.1Q) is extended by 4 bytes, with 12 bits available for recording the VLAN ID. The VLAN IDs "0" and "4095" are reserved and cannot be used for VLAN identification.

**VPN (Virtual Private Network)**

A Virtual Private Network (VPN) connects several separate private networks (partial networks) together via a public network (e.g. the Internet) to form a single joint network. A cryptographic protocol is used to ensure confidentiality and authenticity. A VPN thus offers an economical alternative to using dedicated lines to build a nationwide corporate network.

## 9 Technical Data

### General

<b>CPU</b>	Intel IXP 42x with 266 MHz or 533 MHz
<b>Memory</b>	16 MB Flash, 64 MB SDRAM; mGuard delta: 128 MB
<b>LAN and WAN interfaces</b>	Ethernet IEEE 802 10/100 Mbps RJ45
<b>Serial</b>	RS 232
<b>Power supply</b>	smart: Via USB interface (5 V, 500 mA) or external power supply (110 - 230 V) delta: 5 V DC, 3A
<b>Operating system</b>	Innominate Embedded Linux
<b>Operation supervision</b>	Watchdog and LEDs
<b>Relative humidity</b>	blade, smart, PCI: max. 90% (non-condensing) delta: 5-95% (non-condensing)
<b>Ambient temperature</b>	smart, blade, delta: 0-40 °C PCI: 0-70 °C

### mGuard industrial RS

<b>Network size</b>	Length of a 10BASE-T/100BASE-TX twisted pair segment (approx. 100 m)
<b>Operating voltage</b>	9 to 36 V DC; maximum transient overvoltage 1500 V
<b>Potential difference between input voltage and housing</b>	36 V DC
<b>Power consumption</b>	Maximum 4 W at 24 V DC
<b>Current overload protection at input</b>	Non-changeable fuse
<b>Dimensions</b>	45 mm x 100 mm x 111 mm (W x H x D)
<b>Weight</b>	250 g
<b>Ambient temperature</b>	Ambient air 0 °C to + 55 °C
<b>Relative humidity</b>	10% to 95% (non-condensing)
<b>Pollution degree</b>	2

<b>EMC anti-interference level</b>	Discharge of static electricity Contact discharge: EN 61000-4-2 Air discharge: EN 61000-4-2 Electromagnetic fields: EN 61000-4-3 Fast transients: EN 61000-4-4 Symmetrical surge voltage: EN 61000-4-5 Asymmetrical surge voltage: EN 61000-4-5 Cable-based RF faults: EN 61000-4-6  All entries are determined using test levels that are required for programmable logic controllers (PLCs) used in industrial zone B surroundings (according to EN 61131-2:2003).
<b>EMC emitted immunity</b>	EN 55022:2006: Class A CFR 47 FCC Part 15 (2005-4): Class A
<b>Resistance</b>	Vibration test, sinusoidal according to EN 61131-2:2003 and DIN EN 60068-2-6:1996 (Test parameter according to point 4.2.1 “Vibrations” and 6.2.1 “Vibration test under normal operating conditions” of EN 61131-2:2003) Shock test according to EN 61131-2:2003 and DIN EN 60068-2-27:1996 (Test parameter according to point 4.2.2 “Shocks” and 6.2.1 “Shocks (type test under normal operating conditions)” of EN 61131-2:2003)
<b>Certifications</b>	CE, FCC

## EAGLE mGuard

<b>Network size</b>	Length of a 10BASE-T/100BASE-TX twisted pair segment (approx. 100 m)
<b>Operating voltage</b>	NEC class 2 power source 12VDC or 9.6VDC - 60VDC, or 18VAC - 30VAC Safety extra-low voltage (SELV/PELV, decoupled redundant entries), max. 5A. Buffer time: Min 10 ms at 24 V DC
<b>Potential difference between input voltage and housing</b>	Potential difference to input voltage +24 V DC: 32 V DC Potential difference to input voltage, ground: -32 V DC
<b>Power consumption</b>	Max. 7.2 W at 24 V DC; 24.6 Btu (IT)/h
<b>Current overload protection at input</b>	Non-changeable fuse
<b>Dimensions</b>	W x H x D: 46 mm x 131 mm x 111 mm
<b>Weight</b>	340 g
<b>Ambient temperature</b>	Ambient air 0 °C to +55 °C

<b>Storage temperature</b>	Ambient air -40 °C to +80 °C
<b>Relative humidity</b>	10% to 95% (non-condensing)
<b>Atmospheric pressure</b>	Suitable for operation up to 2000 m (795 hPa)
<b>Pollution degree</b>	2
<b>EMC anti-interference level</b>	<p>Discharge of static electricity</p> <p>    Contact discharge: EN 61000-4-2: Test level 3</p> <p>    Air discharge: EN 61000-4-2: Test level 3</p> <p>Electromagnetic fields: EN 61000-4-3: Test level 3</p> <p>Fast transients: EN 61000-4-4: Test level 3</p> <p>Symmetrical surge voltage: EN 61000-4-5: Test level 2</p> <p>Asymmetrical surge voltage: EN 61000-4-5: Test level 3</p> <p>Cable-based RF faults: EN 61000-4-6: Test level 3</p>
<b>EMC emitted immunity</b>	<p>EN 55022: Class A</p> <p>FCC 47 CFR Part 15: Class A</p> <p>Germanischer Lloyd: Rules for Classification and Construction VI-7-3, part 1, Ed. 2003</p>
<b>Resistance</b>	<p><u>Vibration</u></p> <p>EC 60068-2-6 Test FC: Test level according to IEC 61131-2 E2 CDV and</p> <p>Germanischer Lloyd Guidelines for the Performance of Type Tests, Part 1</p> <p><u>Shock</u></p> <p>EC 60068-2-27 Test EA: Test level according to IEC 61131-2 E2 CDV</p>
<b>Certifications</b>	<p>Complies with cUL 508 / CSA 22.2 No. 142</p> <p>cUL 1604 / CSA 22.2 No. 213 pending</p> <p>Complies with Germanischer Lloyd standards</p>

**Notes on CE identification**

The declarations of conformity are kept available for the responsible authorities in accordance with the EU directives at:

Innominate Security Technologies AG  
Albert-Einstein-Str. 14  
D-12489 Berlin  
Telephone ++49 (0)30 6392-3300

**FCC Note**

This equipment has been tested and complies with the limits for a Class A digital device, according to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at their own expense.